Grant Agreement No.: 101095542
Call: HORIZON- HLTH-2022-IND-13
Topic: HORIZON-HLTH-2022-IND-13-01
Type of action: HORIZON-RIA

CYLCOMED

Cyber-security toolbox
for connected medical devices

D7.3 Dissemination, Communication, Standardisation and Exploitation Initial Report

Revision: v.1.0

Work package	WP7
Task	Task 7.1, 7.2, 7.3, 7.4, 7.5
Due date	31/05/2024
Submission date	31/05/2024
Deliverable lead	MARTEL
Version	1.0
Authors	Jill Blocker (MARTEL), Ricardo Ruiz Fernandez (RGB)

Reviewers	Dietmar Frey (CUB) Orhun Utku Aydin (CUB)

Abstract	This deliverable presents the comprehensive strategy and plan for dissemination, communication, standardisation, and exploitation within the CYLCOMED project. The deliverable also emphasises the project's engagement in standardisation activities and outlines the project's exploitation objectives, including the development of an exploitation strategy, market analyses, and identification of key exploitable results.
Keywords	Exploitation strategy, market analyses, and identification of key exploitable results

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	28/03/2023	ToC Communication and dissemination	Valentin Popescu (Martel)
V0.2	14/04/2023	ToC Standardisation and Exploitation	Ricardo Ruiz Fernandez (RGB)
V0.3	18/04/2023	Content for Communication and dissemination section	Valentin Popescu and Jill Blocker (Martel)
V0.4	16/05/2023	Content for Standardisation and Exploitation section	Ricardo Ruiz Fernandez (RGB)
V0.5	17/05/2023	Integration of content and preparation for internal review	Jill Blocker (Martel)
V0.6	30/05/2023	Internal Review	Orhun Aydin (CUB)
V1.0	31/05/2023	Review and Finalization	Dietmar Frey (CUB)

Disclaimer

The information, documentation and figures available in this deliverable are written by the "Cyber security toolbox for connected medical devices" (CYLCOMED) project’s consortium under EC grant agreement 101095542 and do not necessarily reflect the views of the European Commission.

Funded by Horizon Europe
Framework Programme of the European Union

The European Commission is not liable for any use that may be made of the information contained herein.

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Funded by Horizon Europe Framework Programme of the European Union

Executive summary

This report presents the communication and dissemination activities of the CYLCOMED project during the reporting period (M01-M18). The deliverable focuses on the project's activities related to disseminating project outcomes, communicating project progress, engaging in standardisation activities, and developing an exploitation plan for the project results.

The partners have engaged in various communication and dissemination activities, such as participating in local and international events, publishing scientific papers, sharing news through institutional channels, and promoting the project on social media platforms.

The deliverable highlights the comprehensive dissemination and communication activities that are being undertaken by the CYLCOMED project to maximise the impact and reach of its cybersecurity framework for Connected Medical Devices.

T7.3 –Standardisation Initiatives (M1-M36). Leader: RGB. Contributors: FHUNJ

This task will plan and implement all the actions needed to interact with standardisation bodies for which results obtained in CYLCOMED can be an opportunity to influence ongoing developments in standardisation efforts being conducted by the identified bodies. Some CYLCOMED partners are active in several standards which detail the industrial implementation of regulations and can therefore contribute with novel approaches, particularly in what concerns the interaction and coordination between safety, security and privacy of CPSs. An initial identification of relevant standards and corresponding application domains addressed in CYLCOMED will be delivered in the first months of the project. This will be the baseline identification that will be refined under this task, and from which an initial and final plan of standardisation activities will be derived and implemented during the project time-frame. Standardisation Information will be disseminated information among project partners about certain standards of interest (EN ISO 14971, EN ISO 27779, ISO/IEC 27002 and IEC TR 60601-4-5, EN 62304, EN ISO 14971, EN 60601-1 and EN 60601-1-10. In case contribution from CYLCOMED´s research outcomes for CEN ISO/IEEE 11073 can be of interest for covering security gaps, potential interactions with CEN/ TC 251 will be sought.

T7.2 – Exploitation and IPR management (M1-M36). Leader: RGB. Contributors: All

This task will be dedicated to the exploitation actions partners are expected to complete focused on the commercial viability of the main outcomes. It will consider new business and operating models for bringing the project results to customers considering how obligations under the new Medical Device Regulations can act as catalyst to drive demand for cybersecurity tools (covering risk management and security controls) that CYLCOMED will deliver as project results. This task will put a strong focus on how all stakeholders can profit from the exploitation of the results, and develop a timeline for exploitation, identifying the prospective time frame after the end of the project to bring the results to the market. It will manage the IPR, knowledge management and business planning. CYLCOMED, as a research and innovation project, will explore different types of output:

1) Increased knowledge and expertise which produces “competency impacts”;

2) New or increased knowledge that affects the future performance of the related industries;

Funded by Horizon Europe Framework Programme of the European Union

3) Results which could lead to direct economic benefits (development, creation and marketing of products, services or processes).

4) The Exploitation Leader (RGB), with the support of all partners, will set up a catalogue of the CYLCOMED results and an exploitation plan at the mid- term of the project, which will be updated at the end of the project.

Identification of necessary subsequent research projects, and opportunities for co-funding (at European or National Levels) will be investigated by partners for each Key Exploitable Result identified.

Overall, the CYLCOMED project is engaging in communication and dissemination efforts, creating valuable connections and collaborations with other projects and initiatives in the field of cybersecurity for Connected Medical Devices.

Funded by Horizon Europe
Framework Programme of the European Union

Table of contents

Funded by Horizon Europe Framework Programme of the European Union

Funded by Horizon Europe Framework Programme of the European Union

List of figures

Funded by Horizon Europe Framework Programme of the European Union

List of tables

Funded by Horizon Europe
Framework Programme of the European Union

Abbreviations

ANSI	American National Standards Institute
AI	Artificial Intelligence
CAL	Cybersecurity Assurance Level
CEN	Comité Européen de Normalisation. *English:* European Committee for Standardization
CMD	Connected Medical Device
CPS	Cyber-Physical Systems
CS	CyberSecurity
D	Deliverable
GDPR	General Data Protection Regulation
FDA	Food and Drug Administration
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMDRF	International Medical Device Regulators Forum
ISO	International Organization for Standardization
IVDR	In Vitro Diagnostic Medical Devices Regulation
KPI	Key Performance Indicator
MDCG	Medical Device Coordination Group
MDD	Medical Devices Directive
MDR	Medical Device Regulation
NIS	Network and Information Systems
RAMS	Reliability, Availability, Maintainability, Safety
RMI	Repair and Maintenance Information
RoSPAV	Report on standardisation prospective for automated vehicles
SAMD	Software as a Medical Device
SCP	Safety, Cybersecurity and Privacy
SDO	Standards Development Organization
SME	Small and Medium Enterprises
TAF	Target Attack Feasibility
TC	Technical Committees
TF	Task Force
UL	Underwriters Laboratories
V&V	Verification and Validation

Funded by Horizon Europe
Framework Programme of the European Union

1 INTRODUCTION

The Dissemination and Communication Report for the reporting period ending in M18 (May 2024) presents an intermediate report of the communication and dissemination activities of the CYLCOMED project.

During the reporting period (M01 to M18) of the project, WP7 has been dedicated to defining, coordinating and implementing an extensive set of dissemination and communication activities to amplify project and community building efforts through a rich set of tools and actions for awareness creation and engagement of stakeholders.

1.1 Purpose of the document

This deliverable expands upon the strategic framework established in Deliverable 7.1 “Dissemination and Communication” Strategy and Plan that aims to achieve the following objectives:

- Define a well-articulated communication and dissemination strategy that will increase awareness of CYLCOMED vision, objectives and achievements.
- Set the overall framework, giving direction to media, online, publications, liaisons and communications activities, updated as needed to better match with the specific needs and opportunities.
- Serve all the other CYLCOMED work packages, along with the establishment, maintenance and delivery of the proper tools and means for promotion and impact creation.
- Deliver and be in charge of (1) CYLCOMED visual identity and promo kit; (2) CYLCOMED website and social media channels; (3) Promo materials design and production; (4) Newsletter/news with regular updates; (5) Dissemination through research publications and presentations at conferences, workshops and relevant scientific, domain-related, exhibitions and EC-driven events; (6) Trainings

The report focuses on the key actions carried out during the communication phase through M18. This phase aimed to proactively engage target stakeholders, generate interest in CYLCOMED activities and outcomes, and establish a robust foundation for the planned dissemination activities.

1.2 Structure of the document

The sections of the deliverable at hand are organised in the following manner:

- Section 1 gives the Introduction and overview, with a summary of the main objectives for communication and dissemination for this phase.
- Section 2 presents the various types of communication and dissemination activities and tools used in order to support the project’s dissemination and communication activities.
- Section 3 describes CYLCOMED’s synergies and interaction with external initiatives.
- Section 4 describes the plan for the next phase of the project
- Section 5 depicts the metrics for the evaluation of the dissemination and communication activities.
- Section 6 concludes the document and presents the most relevant next steps.

Funded by Horizon Europe Framework Programme of the European Union

2 COMMUNICATION AND DISSEMINATION

2.1 Dissemination and Communication Objectives

The main aim of CYLCOMED is to deliver an evidence-based comprehensive methodological and technical cybersecurity framework designed for health solutions relying on CMDs. As the healthcare sector becomes more connected, the large volumes of data stored and maintained in healthcare organisations get increasingly exposed to cybersecurity risks for organisations and patients alike. CYLCOMED puts forward the vision of trustworthy, dependable and cost-effective health services and medical care delivered thanks to CMDs for near real-time and/or remote data sharing.

WP7 leads a set of dedicated dissemination and communication actions with the following objectives:

- Define, coordinate and implement an extensive set of dissemination and communication activities to amplify project and community building efforts through a rich set of tools and actions for awareness creation and engagement of stakeholders. This is crucial for effective and sustainable impact creation, as well as for exploitation. The main work package objectives break down as follows
- Develop a robust, agile, and responsive audience-led communication strategy, including an adaptable and engaging website suitable for a range of audiences, to create awareness about project results and stimulate engagement of related stakeholders.
- Facilitate the exploitation of the project's outcome and actively promote the further development of innovative solutions based on the CYLCOMED outcomes both for partners and for other EU players.
- Monitor relevant standardisation initiatives linked to the project and contribute to relevant Standards Development Organisations and/or pre-standardisation groups as relevant and make standardisation contributions.
- Organise and promote special training events for the adoption of the cybersecurity solution developed in CYLCOMED, dedicated to the target stakeholders (manufacturers and suppliers of medical devices, health care providers, patient groups and citizens)

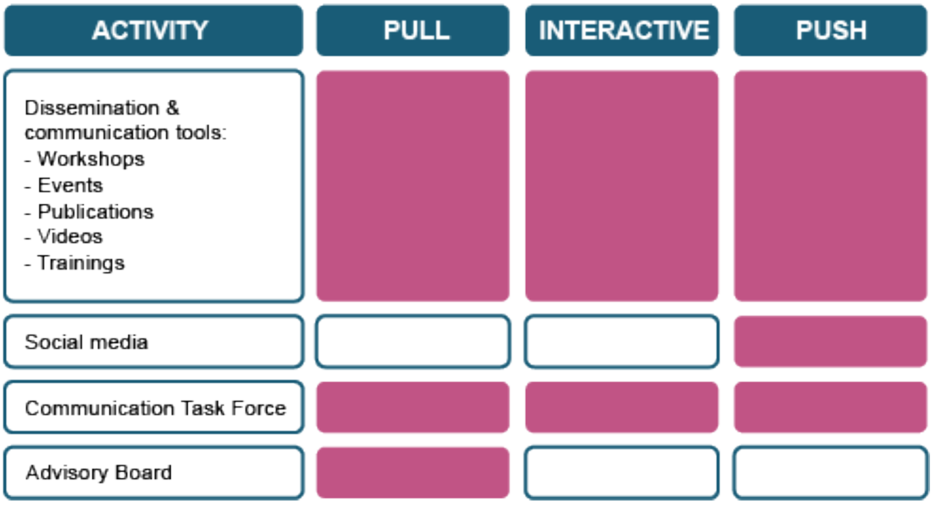
2.2 CYLCOMED target stakeholders

Throughout the activities performed in the reporting period, CYLCOMED has collaborated with a large community of target stakeholders such as:

- **Cybersecurity industry group**
- **Related domains' industry group**
- **Research communities' group**
- **H2020 projects group**
- **Products and service providers group**
- **Standardisation bodies initiatives group**
- **Policy makers**
- **Citizens and civil society**

2.3 COMMUNICATION AND DISSEMINATION IN ACTION

In order to engage with its target audience and stakeholders, CYLCOMED employs a diverse range of communication and dissemination methods. The CYLCOMED website serves as the primary information hub for the community, while social media channels, newsletters, news articles, blogs, and curated stories are also utilised. Content is strategically shared through specialised channels to maximise reach.



ACTIVITY	PULL	INTERACTIVE	PUSH
Dissemination & communication tools: - Workshops - Events - Publications - Videos - Trainings	●	●	●
Social media			●
Communication Task Force	●	●	●
Advisory Board	●		

Figure 1: The communication activities and their relations to the communication and dissemination mix

2.4 Web Portal

The fully functional CYLCOMED website (https://www.cylcomed.eu/) represents the entry point that enables the project to reach all stakeholders involved. All relevant information about projects, outcomes, events, milestones, developments, etc., are exposed and accessible via the dedicated areas the portal has been structured around.

The website has a clear and clean communication interface that is easily navigable, containing all relevant project related public information. The website also offers direct access to the most relevant documents produced by the consortium.

Since its launch, the website has been updated, and the content improved with regular updates including:

- **About CYLCOMED** https://www.cylcomed.eu/cylcomed/
- **Use Cases (1&2):** https://www.cylcomed.eu/use-case-1/, https://www.cylcomed.eu/use-case-2/
- **News:** https://www.cylcomed.eu/news/
- **Events:** https://www.cylcomed.eu/all-events/
- **Blog section**: https://www.arcadian-iot.eu/blog/
- **Resources**
    - **Deliverables:**https://www.cylcomed.eu/deliverables/
    - **Publications:** https://www.cylcomed.eu/publications/
    - **Presentations:** https://www.cylcomed.eu/presentations/
    - **Press Releases:** https://www.cylcomed.eu/press-releases/

During the reporting period, several news items were published on the website:

Funded by Horizon Europe Framework Programme of the European Union

- Cybersecurity for Medical Devices – a preliminary legal and ethical analysis https://www.cylcomed.eu/cybersecurity-for-medical-devices-a-preliminary-legal-and-ethical-analysis/
- Meet The CYLCOMED Partner: EVIDEN, an Atos business https://www.cylcomed.eu/meet-the-cylcomed-partner-eviden-an-atos-business/
- Horizon Europe Projects Partnership to Improve Cybersecurity of CMDs: https://www.cylcomed.eu/horizon-europe-projects-partnership-to-improve-cybersecurity-of-cmds/
- Meet the CYLCOMED Partner: KU Leuven https://www.cylcomed.eu/meet-the-cylcomed-partner-ku-leuven/
- Researchers, healthcare and technology providers start collaboration to boost cybersecurity for connected medical devices https://www.cylcomed.eu/researchers-healthcare-and-technology-providers-start-collaboration-to-boost-cybersecurity-for-connected-medical-devices/
- CYLCOMED Project kicks off in Madrid https://www.cylcomed.eu/cylcomed-project-kicks-off-in-madrid/

CYLCOMED website analytics

In the reporting period (January 2022 - May 2023), the CYLCOMED website had 1,369 unique visitors and 3,267 page views.

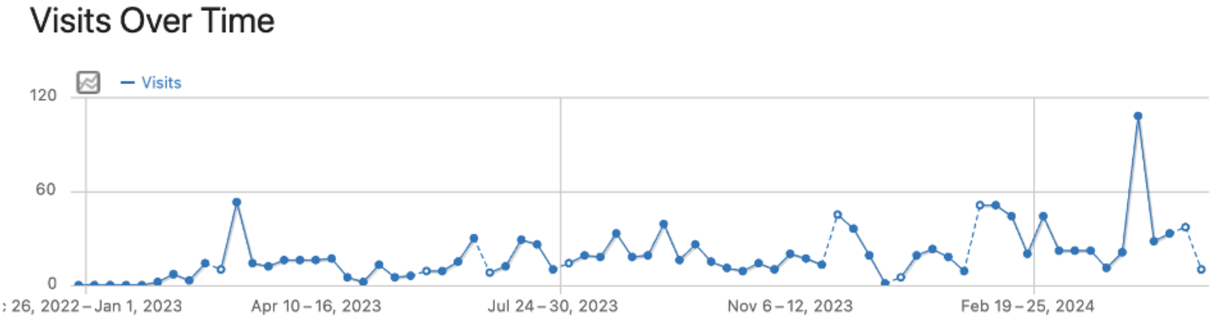
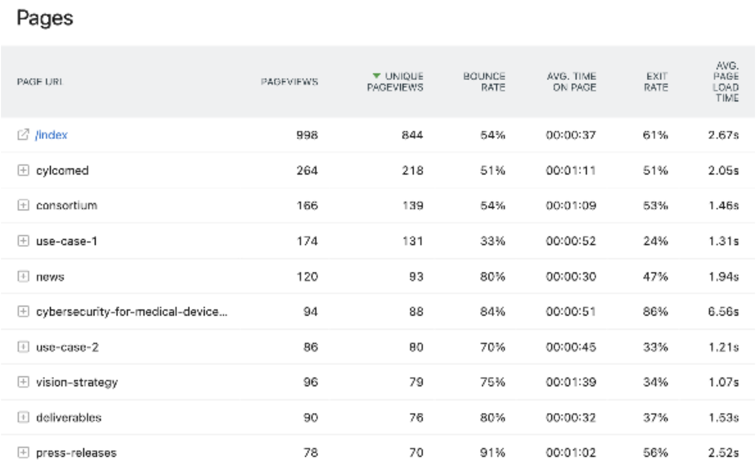


Figure 2: Website analytics for lifetime, Jan. 2023-May2024

The most visited pages of the website are the homepages, information about the consortium, news publications and case studies.



Pages

PAGE URL	PAGEVIEWS	▼ UNIQUE PAGEVIEWS	BOUNCE RATE	AVG. TIME ON PAGE	EXIT RATE	AVG. PAGE LOAD TIME
/index	998	844	54%	00:00:37	61%	2.67s
⊞ cylcomed	264	218	51%	00:01:11	51%	2.05s
⊞ consortium	166	139	54%	00:01:09	53%	1.46s
⊞ use-case-1	174	131	33%	00:00:52	24%	1.31s
⊞ news	120	93	80%	00:00:30	47%	1.94s
⊞ cybersecurity-for-medical-device...	94	88	84%	00:00:51	86%	6.56s
⊞ use-case-2	86	80	70%	00:00:45	33%	1.21s
⊞ vision-strategy	96	79	75%	00:01:39	34%	1.07s
⊞ deliverables	90	76	80%	00:00:32	37%	1.53s
⊞ press-releases	78	70	91%	00:01:02	56%	2.52s

Figure 3: Website Pageviews for lifetime, Jan. 2023-May2024

Funded by Horizon Europe Framework Programme of the European Union

The most visits are from Spain, Switzerland, Germany and Italy, with the majority of visits from Europe, followed by the United States and Asia.

Based on the provided analytics data for the CYLCOMED website for the period of January 2022 to May 2024, we have the following traffic sources:

- **Direct: 955 (70%):** Direct traffic occurs when users type the website's URL directly into their browser's address bar, access it through browser bookmarks, or click on a link in an email or a document (e.g., a PDF). This traffic source often reflects users who are already familiar with the project or have visited the website before.
- **Organic Search: 224 (16%):** Organic search traffic refers to users who found the website through a search engine (e.g., Google, Bing, Yahoo) by entering relevant keywords.
- **Social: 122 (9%):** Social traffic comes from users who find and visit the website through social media platforms (e.g., Facebook, X, LinkedIn, Instagram).
- **Referral: 68 (5%):** Referral traffic is generated when users visit the website by clicking on a link from another website. This can include links in blog posts, news articles, or online directories.

Measures to improve website traffic:

1. **Enhance Organic Search Traffic:** Organic search accounts for 16% of the total traffic, indicating that there is significant room for improvement. To boost organic search traffic, we will focus on:
    - Conducting thorough keyword research and incorporating relevant keywords into your website's content.
    - Improving on-page SEO by optimising metadata (title tags, meta descriptions, header tags, etc.) and creating high-quality, informative content that engages visitors.
    - Utilising internal and external links to improve site navigation and build a strong backlink profile.
    - Regularly updating and maintaining your website to ensure optimal performance and user experience.
2. **Strengthen Social Media Presence:** Social media contributes 9% of the total traffic, indicating potential growth in this area. To increase social traffic, we will consider:
    - Developing a consistent and engaging social media strategy that includes regular content updates, audience engagement, and promotion of the website.
    - Leveraging various social media platforms such as Twitter and LinkedIn to reach a wider audience.
    - Creating shareable content (e.g., blog posts, infographics, videos) to encourage our audience to share your content on their social media profiles.
3. **Boost Referral Traffic:** With referrals accounting for only 5% of the total traffic, there's room to increase this metric. To enhance referral traffic, we will consider:
    - Establishing partnerships with relevant industry websites, blogs, or online communities.
    - Engaging in guest posting on authoritative websites in your niche.
    - Offering valuable resources, such as whitepapers or webinars, that can be shared by other websites.

4. **Direct Traffic:** Direct traffic constitutes the majority of the website's traffic (70%). It is important to understand the source of this traffic and identify potential growth opportunities. We will consider:
    - Ensuring that your website is easily accessible through clear navigation, fast loading times, and mobile-friendly design.
    - Encouraging repeat visitors by offering valuable content.

By focusing on these recommendations, you can work towards a more balanced traffic acquisition strategy and increase the overall performance of the CYLCOMED website.

2.4 Social Media

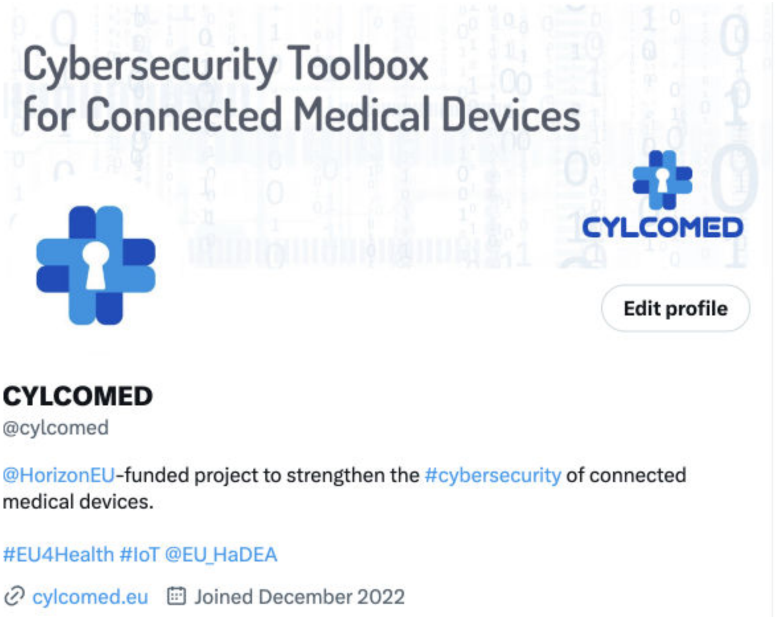
X (formerly Twitter), LinkedIn and Youtube social media channels were established as communication tools in order to promote activities and outputs of the project on a regular basis, while also encouraging a wider discussion on the topics related to the project’s activities. So far, CYCLOMED created an active presence on the most popular social media channels, such as Twitter and LinkedIn, which are linked to the project's website. In addition, the YouTube channel was opened, and it features videos of training sessions and will host videos of events where CYCLOMED was presented, interviews with the consortium partners and animated video showcasing the use cases.

2.4.1 X (formerly Twitter)

CYLCOMED established its Twitter account @CYLCOMED (https://twitter.com/cylcomed) in December 2022 and since then has used the social medium to inform and engage the relevant audience and create awareness about the project.

The Twitter account is used for promoting and disseminating the development of CYLCOMED, including news, events, outcomes, etc. Moreover, replies are made of relevant and interesting content from disparate sources.

By the time of writing this report, CYCLOMED has 142 followers and has a total of 46 posts. posted, on average, one tweet a week, beside the regular retweets from other followed accounts.



CYLCOMED
@cylcomed

@HorizonEU-funded project to strengthen the #cybersecurity of connected medical devices.

#EU4Health #IoT @EU_HaDEA

cylcomed.eu Joined December 2022

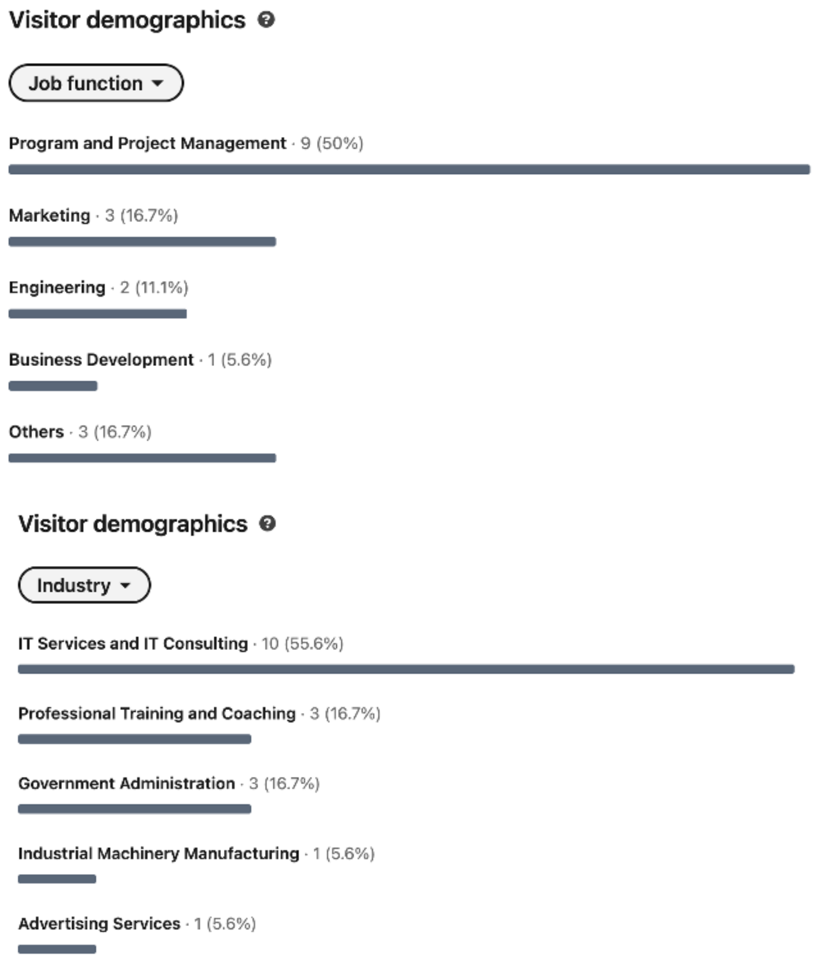
Figure 4: CYLCOMED X (Twitter) account

2.4.2 LinkedIn

LinkedIn is a business-oriented professional networking tool that is used by many as a source of information and inspiration, therefore, it serves as a solid tool to amplify the news shared on the website. It is an important platform for discussions relevant to CYCLOMED, among experts in the area and various stakeholders in general.

The CYCLOMED LinkedIn page (https://www.linkedin.com/company/cylcomed) allows reaching a professional audience with more elaborated news and/or specific events highlights. The page was established in May 2023, ahead of the project's start, and has at the time of writing this report (May 2024) 47 followers.

Below, a few key figures regarding the LinkedIn account:



Visitor demographics

Job function

Program and Project Management · 9 (50%)

Marketing · 3 (16.7%)

Engineering · 2 (11.1%)

Business Development · 1 (5.6%)

Others · 3 (16.7%)

Visitor demographics

Industry

IT Services and IT Consulting · 10 (55.6%)

Professional Training and Coaching · 3 (16.7%)

Government Administration · 3 (16.7%)

Industrial Machinery Manufacturing · 1 (5.6%)

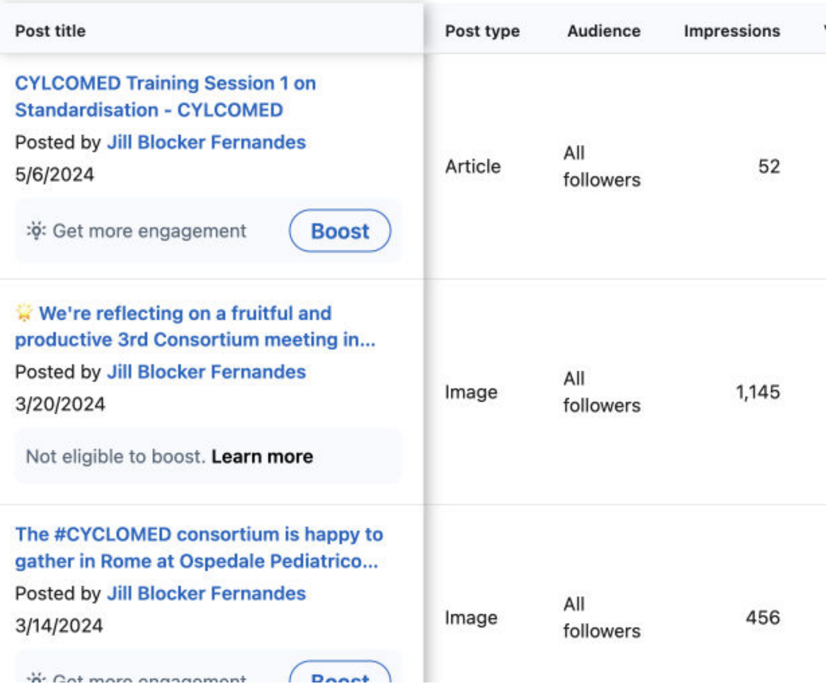
Advertising Services · 1 (5.6%)

Figure 5: Industries and functions of the visitors of CYLCOMED LinkedIn account

Funded by Horizon Europe Framework Programme of the European Union

During the reporting period, the Linkedin page had over 3,200 impressions.

Based on the analytics provided by LinkedIn, the most engaging content are images and blog posts. As such, we will continue to create this kind of content and promote it on this social network.



Post title	Post type	Audience	Impressions
CYLCOMED Training Session 1 on Standardisation - CYLCOMED Posted by Jill Blocker Fernandes 5/6/2024 Get more engagement Boost	Article	All followers	52
We're reflecting on a fruitful and productive 3rd Consortium meeting in... Posted by Jill Blocker Fernandes 3/20/2024 Not eligible to boost. **Learn more**	Image	All followers	1,145
The #CYCLOMED consortium is happy to gather in Rome at Ospedale Pediatrico... Posted by Jill Blocker Fernandes 3/14/2024 Get more engagement Boost	Image	All followers	456

Figure 5: Impression report of CYLCOMED LinkedIn account

2.5 Publications, Presentations and Talks

The CYLCOMED team has had the opportunity to publish in scientific journals and conference publications, with the following publications:

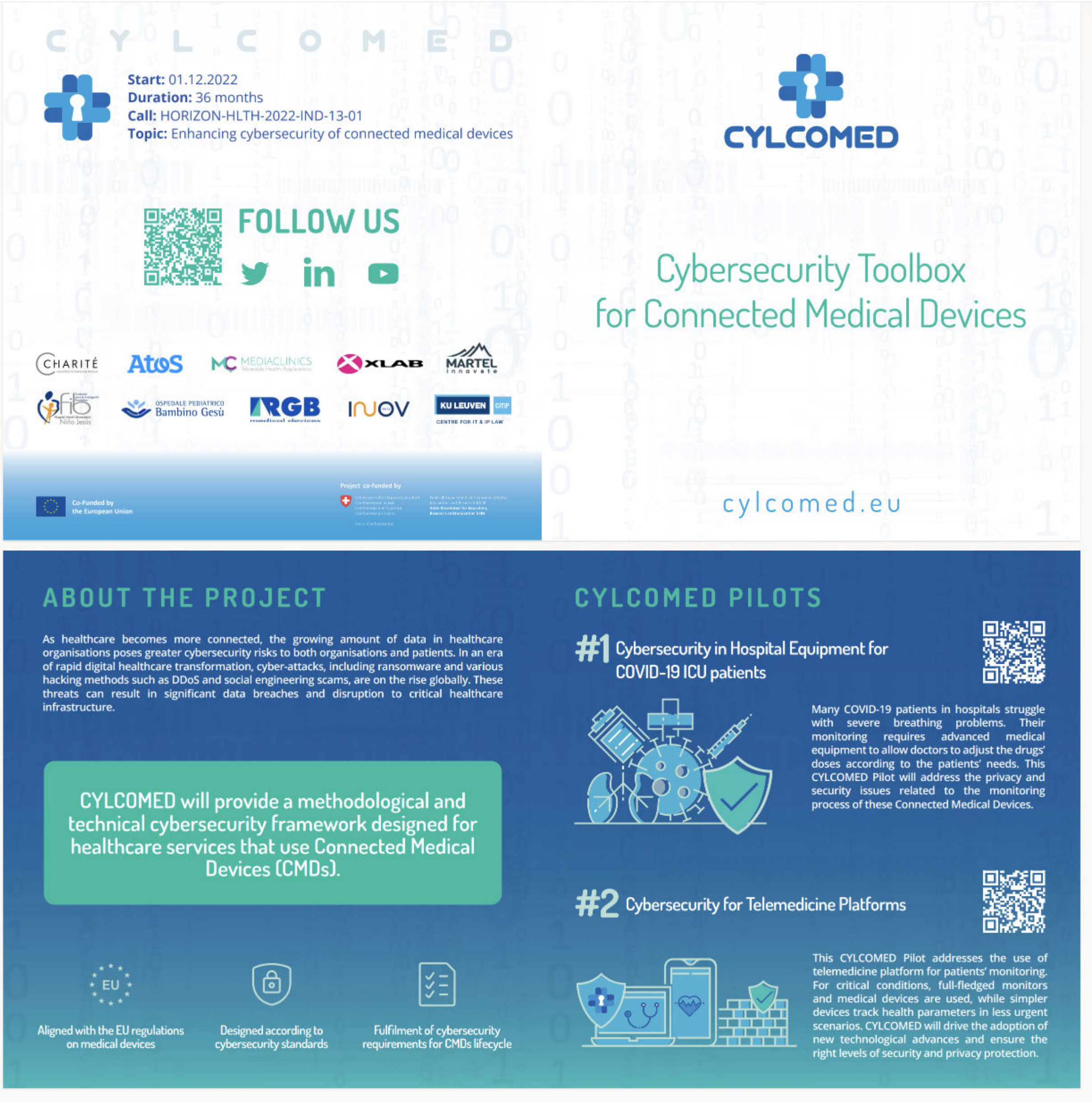
- "CYLCOMED for Cybersecurity for Connected Medical Devices: Raising cybersecurity to a new level," by Dusko Milojevica and Maja Nisevicb.
- "Legal Challenges in the Internet of Medical Things (IoMT) in the EU," by Dusko Milojevic in the journal, Eleventh Annual Governance of Emerging Technologies and Science Conference.
- "A Way Forward for the MDCG 2019-16 Medical Device Security Guidance," by Andres Castillo, Dietmar Frey, Simone Favrin, João Rodrigues, Duško Milojević, et al., in the journal, The PErvasive Technologies Related to Assistive Environments (PETRA).
- CYLCOMED was also represented at the Geneva Digital Law Research Colloquium in Geneva, Switzerland on 22 June 2023 by Maja Nisevic of KU Leuven in a presentation titled, "Using AI Robots in Medicine: The Interplay Between Technology, Medicine and Law as a gateway for discovering appropriate liability regime."
- Additionally, a tutorial titled, "Reputation Systems in 5G/6G Networks," by Bruno Sousa in the Journal, IEEE IF/IP NOMS 2024 is prepared for publication.

Funded by Horizon Europe Framework Programme of the European Union

- **XLAB** has also prepared a paper submission entitled “LOMOS: an AI-based runtime security monitoring system fit for the cloud continuum” for the Euro-PAR 2024 Conference including the CYLCOMED partners XLAB and MediaClinics.
- Finally, contribution from CYLCOMED partners to the Workshop paper for the PETRA Conference has been accepted and is going to be published as open-source publication.

2.6 Promotional Material

With the resumption of events with physical presence, the consortium produced promotion materials to be used and distributed. Flyers are available for the promotion of the project among the participants.



CYLCOMED

Start: 01.12.2022
Duration: 36 months
Call: HORIZON-HLTH-2022-IND-13-01
Topic: Enhancing cybersecurity of connected medical devices

FOLLOW US

CHARITÉ
AtoS
MC MEDIACLINICS
XLAB
MARTEL innovate
fib Niño Jesús
OSPEDALE PEDIATRICO Bambino Gesù
RGB medical devices
INOV
KU LEUVEN CITIP CENTRE FOR IT & IP LAW

Co-Funded by the European Union

Project co-funded by

CYLCOMED

Cybersecurity Toolbox for Connected Medical Devices

cylcomed.eu

ABOUT THE PROJECT

As healthcare becomes more connected, the growing amount of data in healthcare organisations poses greater cybersecurity risks to both organisations and patients. In an era of rapid digital healthcare transformation, cyber-attacks, including ransomware and various hacking methods such as DDoS and social engineering scams, are on the rise globally. These threats can result in significant data breaches and disruption to critical healthcare infrastructure.

CYLCOMED will provide a methodological and technical cybersecurity framework designed for healthcare services that use Connected Medical Devices (CMDs).

Aligned with the EU regulations on medical devices

Designed according to cybersecurity standards

Fulfilment of cybersecurity requirements for CMDs lifecycle

CYLCOMED PILOTS

#1 Cybersecurity in Hospital Equipment for COVID-19 ICU patients

Many COVID-19 patients in hospitals struggle with severe breathing problems. Their monitoring requires advanced medical equipment to allow doctors to adjust the drugs’ doses according to the patients’ needs. This CYLCOMED Pilot will address the privacy and security issues related to the monitoring process of these Connected Medical Devices.

#2 Cybersecurity for Telemedicine Platforms

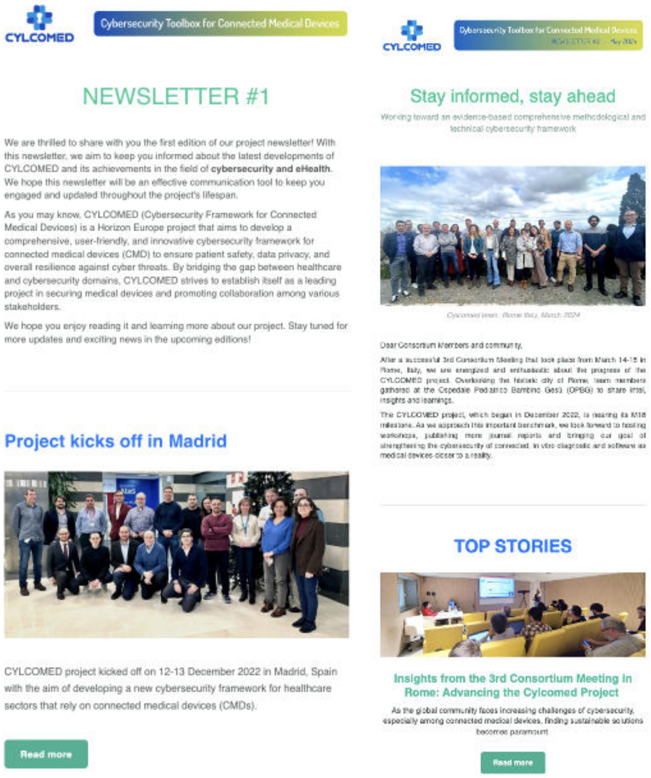
This CYLCOMED Pilot addresses the use of telemedicine platform for patients’ monitoring. For critical conditions, full-fledged monitors and medical devices are used, while simpler devices track health parameters in less urgent scenarios. CYLCOMED will drive the adoption of new technological advances and ensure the right levels of security and privacy protection.

Figure 6: CYCLOMED flyer

Funded by Horizon Europe Framework Programme of the European Union

2.7 Newsletter

CYLCOMED produces e-newsletters on a regular basis, which provide updates on the project, future events, as well as news from project partners and stakeholders upon subscription and news availability. In the reporting period, two editions were developed and distributed. The CYLCOMED e-Newsletters are uploaded to the project website: https://www.cylcomed.eu/newsletter/



CYLCOMED

Cybersecurity Toolbox for Connected Medical Devices

NEWSLETTER #1

We are thrilled to share with you the first edition of our project newsletter! With this newsletter, we aim to keep you informed about the latest developments of CYLCOMED and its achievements in the field of **cybersecurity and eHealth**. We hope this newsletter will be an effective communication tool to keep you engaged and updated throughout the project's lifespan.

As you may know, CYLCOMED (Cybersecurity Framework for Connected Medical Devices) is a Horizon Europe project that aims to develop a comprehensive, user-friendly, and innovative cybersecurity framework for connected medical devices (CMD) to ensure patient safety, data privacy, and overall resilience against cyber threats. By bridging the gap between healthcare and cybersecurity domains, CYLCOMED strives to establish itself as a leading project in securing medical devices and promoting collaboration among various stakeholders.

We hope you enjoy reading it and learning more about our project. Stay tuned for more updates and exciting news in the upcoming editions!

Project kicks off in Madrid

CYLCOMED project kicked off on 12-13 December 2022 in Madrid, Spain with the aim of developing a new cybersecurity framework for healthcare sectors that rely on connected medical devices (CMDs).

Read more

CYLCOMED

Cybersecurity Toolbox for Connected Medical Devices
NEWSLETTER #2 – May 2024

Stay informed, stay ahead

Working toward an evidence-based comprehensive methodological and technical cybersecurity framework

Cylcomed team - Rome Italy, March 2024

Dear Consortium Members and community,

After a successful 3rd Consortium Meeting that took place from March 14-15 in Rome, Italy, we are energized and enthusiastic about the progress of the CYLCOMED project. Overlooking the historic city of Rome, team members gathered at the Ospedale Pediatrico Bambino Gesù (OPBG) to share intel, insights and learnings.

The CYLCOMED project, which began in December 2022, is nearing its M18 milestone. As we approach this important benchmark, we look forward to hosting workshops, publishing more journal reports and bringing our goal of strengthening the cybersecurity of connected, in vitro diagnostic and software as medical devices closer to a reality.

TOP STORIES

Insights from the 3rd Consortium Meeting in Rome: Advancing the Cylcomed Project

As the global community faces increasing challenges of cybersecurity, especially among connected medical devices, finding sustainable solutions becomes paramount

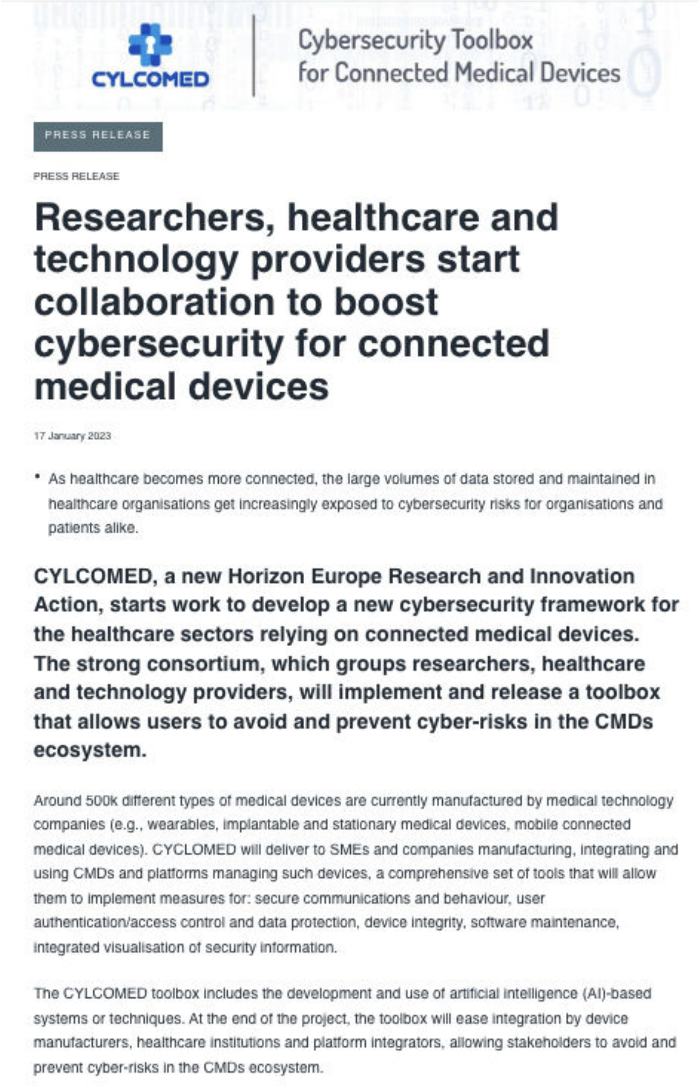
Read more

Figure 7: Snapshots of the CYLCOMED Newsletter

2.8 Media Relations and Engagement

In the reporting period, one press release was distributed. The topic of the press release was the announcement of the project work, titled: "Researchers, healthcare and technology providers start collaboration to boost cybersecurity for connected medical devices." (https://martel-innovate.prowly.com/223276-researchers-healthcare-and-technology-providers-start-collaboration-to-boost-cybersecurity-for-connected-medical-devices)

The press release was distributed to the partners for further dissemination and to journalists Europe-wide on January 17, 2023.



PRESS RELEASE

Researchers, healthcare and technology providers start collaboration to boost cybersecurity for connected medical devices

17 January 2023

- As healthcare becomes more connected, the large volumes of data stored and maintained in healthcare organisations get increasingly exposed to cybersecurity risks for organisations and patients alike.

CYLCOMED, a new Horizon Europe Research and Innovation Action, starts work to develop a new cybersecurity framework for the healthcare sectors relying on connected medical devices. The strong consortium, which groups researchers, healthcare and technology providers, will implement and release a toolbox that allows users to avoid and prevent cyber-risks in the CMDs ecosystem.

Around 500k different types of medical devices are currently manufactured by medical technology companies (e.g., wearables, implantable and stationary medical devices, mobile connected medical devices). CYCLOMED will deliver to SMEs and companies manufacturing, integrating and using CMDs and platforms managing such devices, a comprehensive set of tools that will allow them to implement measures for: secure communications and behaviour, user authentication/access control and data protection, device integrity, software maintenance, integrated visualisation of security information.

The CYLCOMED toolbox includes the development and use of artificial intelligence (AI)-based systems or techniques. At the end of the project, the toolbox will ease integration by device manufacturers, healthcare institutions and platform integrators, allowing stakeholders to avoid and prevent cyber-risks in the CMDs ecosystem.

Figure 8: Snapshot of the CYLCOMED press release

2.9 Events

During the reporting period, CYLCOMED took part in several events, including:

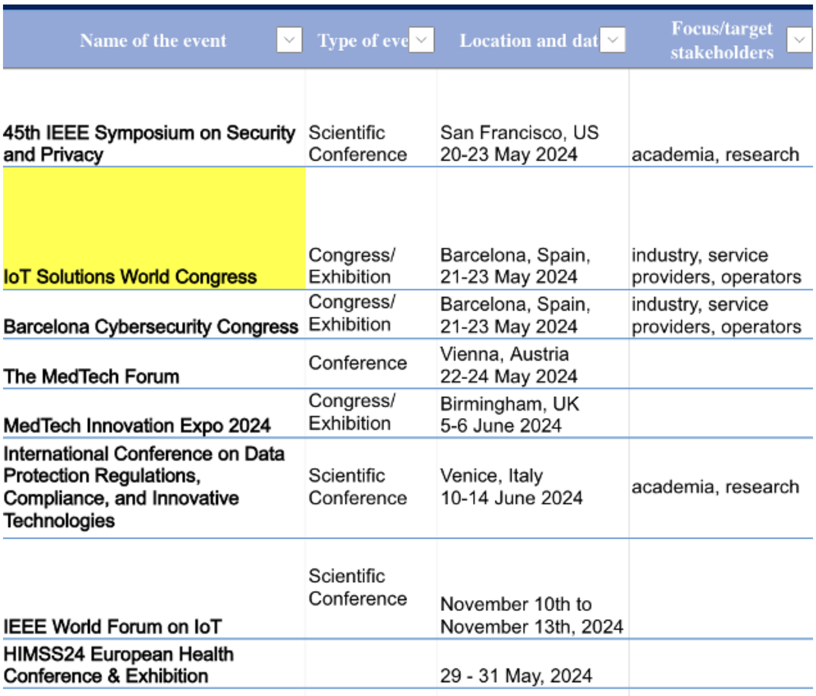
- The Geneva Digital Law Research Colloquium, a Scientific Conference that took place in Geneva Switzerland on 22 June 2023. The focus target stakeholders were academia and researchers. At the event, the partner **KUL** presented and shared a related publication along with **Ospedale Bambino Gesu**'.
- At MEDICA FAIR in Düsseldorf, Germany from November 13-16, 2023, CYCLOMED partner **RGB** had a booth with a screen and distributed flyers about the project to an audience of manufacturers, industry and distributors. MEDICA Trade Fair is the world's largest event for the medical sector. This is the most important international Fair in the world, with over 175.000 visitors.
- CYCLOMED partner **KUL** also participated in the Scientific Conference, ACM Symposium on Computer Science and Law, in Boston, USA from 12-13 March, 2024. Partners KUL, INOV, FHUNJ and Charite' submitted a joint paper.
- GETS Conference in Phoenix Eleventh Annual Governance of Emerging Technologies and Science Conference | ASU Events where **KU Leuven** presented

Funded by Horizon Europe Framework Programme of the European Union

part of the Research conducted under the CYLCOMED project. The topic of the presentation is: Internet of Medical Things Legal Challenges in the EU.

- **KU Leuven** received an invitation from the Vrije Universteite Brussel (VUB) https://www.vub.be/en to deliver a guest talk about CYLCOMED project or other research related to cybersecurity for medical devices. The guest talk is scheduled on 19 Jun. The VUB is currently engaged in a sister project CYMEDSEC (https://cymedsec.eu/), which started in November 2023 under Professor Quinn's supervision.

Additional planned upcoming opportunities include:



Name of the event	Type of eve	Location and dat	Focus/target stakeholders
45th IEEE Symposium on Security and Privacy	Scientific Conference	San Francisco, US 20-23 May 2024	academia, research
IoT Solutions World Congress	Congress/ Exhibition	Barcelona, Spain, 21-23 May 2024	industry, service providers, operators
Barcelona Cybersecurity Congress	Congress/ Exhibition	Barcelona, Spain, 21-23 May 2024	industry, service providers, operators
The MedTech Forum	Conference	Vienna, Austria 22-24 May 2024	
MedTech Innovation Expo 2024	Congress/ Exhibition	Birmingham, UK 5-6 June 2024	
International Conference on Data Protection Regulations, Compliance, and Innovative Technologies	Scientific Conference	Venice, Italy 10-14 June 2024	academia, research
IEEE World Forum on IoT	Scientific Conference	November 10th to November 13th, 2024	
HIMSS24 European Health Conference & Exhibition		29 - 31 May, 2024	

Figure 9: Planned CYLCOMED participation to events

3. Synergies with Other Projects and Initiatives

One of CYLCOMED's goals is to create synergies with other initiatives. To this end, we reached out to other EC-funded projects and organisations, informing them about CYLCOMED's aims and objectives and inviting them to share information on their project with us. Below is a list of the projects approached for collaboration.

The objective for creating these connections is to facilitate a cross dissemination of both actions via shared-blog entries, cross-referral on the project websites, mutual social network interaction and event sharing perspective and to have a constant flow of communication between the initiatives in order to promote additional points for collaboration which may emerge in the short and mid-term.

4. Impact Creation Monitoring

4.1 Communication and Dissemination KPIs

The following metrics are used to monitor and assess the progress of the dissemination and communication activities and provide some measurable outcomes related to their impact created (as far as this is feasible from a quantitative point of view).

Measure	Indicators and Target (M36)	Results at M18
Flyers Posters / roll-ups	*Nº of flyers *:* 6 *Nº of posters/roll-ups *:* 4	1 0
Project Website	*Nº of unique visitors to the website:* 1,500 (average per year)	1,369 visitors
Social Networks	Project accounts on X (Twitter) and LinkedIn: ≥ 1,000 connections/followers in total; ≥ 60 posts on social networks	*Nº followers on X (Twitter):* 142 *Nº followers on LinkedIn: 47* *+60 posts on social networks*
Press Releases* / publication in press*	*Nº of press releases issued to specialised and general media channels:* 6	2 press releases
Videos	*Nº of videos published on the project website and social media:* 6	Nº of videos: 1 in-progress
Participation to events and presentations	*Nº of external events partners attended to promote the project:* at least 4 events per year	
Workshops (2)	*Average Nº of participants: At least 30 participants each*	1 workshop

Funded by Horizon Europe Framework Programme of the European Union

Cybersecurity Training (6, 2 per use case)	*Average Nº of participants:* At least 20 participants each	Planned for later in the project
4 thematic webinars in (M20,24,30,36)	*Average Nº of participants:* At least 50	Planned for later in the project
Scientific publications	*Nº of peer-reviewed publications in journals:* At least 10. *Nº of peer-reviewed publications in conferences and workshops:* At least 14	2 3
Newsletters	*Nº of newsletters: 9 (every 4 months)*	2

Table 2: Dissemination and Communication KPIs

3 STANDARDISATION STRATEGY AND PLAN

3.1 CYLCOMED standardisation mission

The way partners can be related to a specific standard is: i) at system level, e.g., on the tools or methods for the verification of requirements for the implementation of a use case demonstrator, or ii) at component level, e.g., the specific cybersecurity tool that a CYLCOMED partner uses in compliance with a specific standard.

In CYCLOMED we intend to identify and comply with those standards that are more significant for those specific methods and tools developed/ used by partners. The deliverable presents a first study of the standards most related with cybersecurity in the health care domain. Then a plan is presented to learn more about the current development status of applicable standards and discuss possibilities of improvements. Through identification of specific standardisation groups that could be approached and influenced by the project partners, proposals of improvements of those standards will be evaluated based on the results generated by the project partners in the remaining one and a half years of the project.

3.2 CYLCOMED Project compromises

Specific actions proposed:

- Plan and implement all the actions needed to interact with standardisation bodies.
- Detected results obtained in CYLCOMED that can influence ongoing standardisation efforts, particularly in what concerns the interaction and coordination between safety, security and privacy of CPSs.
- Initial identification of relevant standards and corresponding application domains addressed in CYLCOMED, as baseline identification that will be refined under this task.
- From here, an initial plan of standardisation activities follows up what was described in D7.1, to be implemented during the project time-frame.
- Standardisation Information will be disseminated among project partners about certain standards of interest.

As expected results:

- Thorough review of the state of the art for CMD cybersecurity
- Identification of gaps and requirements based on evidence and assessment of the applicability (and revision) of current cybersecurity guidance
- Make recommendations to better address specificities of MDs of different risk classes.
- Number of authoritative sources of standards, guidelines and best practices systematically reviewed in the state of the art; >= 2 iterations of recommendations to (better) address specificities of CMDs;
- Generalisable library of functional and non-functional evidence-based requirements for CMD/IVD/SaMD, contextualised to at least 4 technological trends (AI, 5G, blockchain, cloud computing) and covering 4 different dimensions (safety, effectiveness, security and data protection);

Funded by Horizon Europe Framework Programme of the European Union

- Co-creation of requirements with healthcare end users for medical devices safety, security, privacy and effectiveness related to realistic operational scenarios (>2) and managed over telemedicine platforms (>=1)

3.3 Second review for identification of applicable CMD Cybersecurity standards

3.3.1 Standards with Impact on Cybersecurity

We have been working on reviewing and identifying the main standards that could have a relevant impact on cybersecurity requirements in the Medical domain. The new MDR and IVDR bring EU legislation into line with technical advances, changes in medical science and progress in law-making. We have structured (e.g., considering requirements for manufacturers and operators) summarising key aspects found in MDCG 2019-16 rev. 1 (July 2020) as well as in MDR/IVDR Regulations (especially Annex I), also providing pointers to other relevant regulations (GDPR [30], NIS2, Cybersecurity Act [31]).

- There are not any harmonised standard on cybersecurity, but it is a requirement of 2017/45 regulation
- European Union has issued a guidance on cybersecurity that includes references to relevant standards
- IEC TR 60601-4-5 5 Medical Electrical Equipment – Part 4-5. Safety related technical security specifications for medical devices.. This standard provides detailed technical information for security features in medical devices used in medical IT networks
- ISO 27799 standard gives guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s). By implementing ISO 27799:2016, healthcare organisations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organisation's circumstances and that will maintain the confidentiality, integrity and availability of personal health information in their care.

Up till now, one of our main objectives has been to focus on cybersecurity aspects and:

- Collect, analyse and synthesise project requirements for cybersecurity aspects from a technical, legal, clinical and ethical perspective
- Perform a study of the state of the art regarding the cybersecurity baseline, as to identify gaps and possible areas of improvement
- Define a set of end-user, functional and non-functional requirements for contributing to the future (outside VALU3S scope) overall objective of developing the cybersecurity tools (also in connection with legal and ethical requirements traced in WP2), so that it is user-friendly, trustworthy, reliable and scalable.

3.3.2 Cybersecurity Requirements in the MDR

MDR requests manufacturers of medical devices to consider the state of the art when designing, developing and upgrading medical devices across their life cycle. Manufacturers

Funded by Horizon Europe Framework Programme of the European Union

should demonstrate state-of-the-art within their decisions (based on applicable standards, guidance, their own proprietary knowledge and publicly available scientific/technical information) while demonstrating appropriateness to proportionally address security risk.

Figure XX shows the MDR requirements applied on cybersecurity and other related regulations.

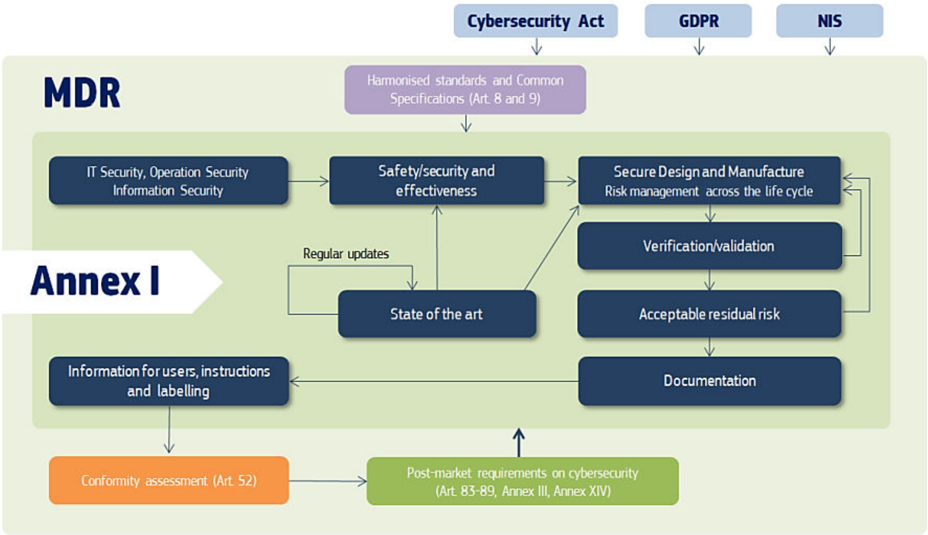

Cybersecurity Act
GDPR
NIS
MDR
Harmonised standards and Common Specifications (Art. 8 and 9)
IT Security, Operation Security Information Security
Safety/security and effectiveness
Secure Design and Manufacture Risk management across the life cycle
Verification/validation
Regular updates
Annex I
State of the art
Acceptable residual risk
Information for users, instructions and labelling
Documentation
Conformity assessment (Art. 52)
Post-market requirements on cybersecurity (Art. 83-89, Annex III, Annex XIV)

Figure 10. MDR Requirements on Cybersecurity

The manufacturer should be particularly aware of the following MDR provisions in the context of cybersecurity:

- Privacy and data protection: Article 62.4(h): General requirements regarding clinical investigations conducted to demonstrate conformity of devices
- Conformity assessment procedures: Article 52
- Post-market surveillance system of the manufacturer: Article 83
- Post-market surveillance plan: Article 84
- Post-market surveillance report: Article 85
- Periodic safety update report: Article 86
- Reporting of serious incidents and field safety corrective actions: Article 87
- Trend reporting: Article 88
- Analysis of serious incidents and field safety corrective actions: Article 89
- Technical documentation: Annex II
- Technical documentation on post-market surveillance: Annex III
- Clinical evaluation and post-market follow-up: MDR Chapter VI and Annex XIV

Figure 10 shows the above listed MDR requirements separated between pre-market and post-market activities.

Table 3. MDR Requirements on Cybersecurity

Pre-market activities	Post-market activities
Secure Design (Annex I)	
Risk management (Annex 1)	Risk management (Annex I)
Establish Risk Control Measures (Annex 1)	Modify Risk Control Measures /Corrective Actions/Patches (Annex 1)
Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex 1)	Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex 1)
Technical Documentation (Annex II and III)	Maintain and update a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84)
Conformity Assessment (Article 52)	Trend Reporting (Article 88)
Establish a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84)	Analysis of Serious Incidents (Article 89)
Clinical evaluation process (Chapter VI)	Post-Market Surveillance Report (Article 85)
	Periodic Safety Update Report (Article 86)
	Update Technical Documentation (Annex II and III)
	Inform the Electronic System On Vigilance (Article 92)

3.3.3 MDR/IVDR General Safety and Performance Requirements

In the EU, both the MDR and IVDR requirements mandate consideration of medical device cybersecurity, and the MDCG 2019-16 guidance directs manufacturers on how to fulfil all the relevant general safety and performance requirements from Annex I of the MDR 2017/745 and IVDR 2017/746 with regard to cybersecurity. Figure 3.6 shows these requirements.

Funded by Horizon Europe Framework Programme of the European Union

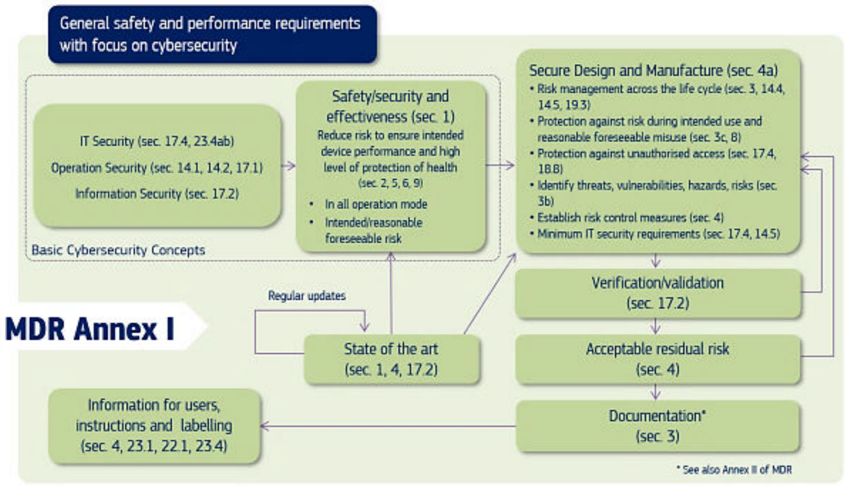

General safety and performance requirements with focus on cybersecurity
IT Security (sec. 17.4, 23.4ab)
Operation Security (sec. 14.1, 14.2, 17.1)
Information Security (sec. 17.2)
Basic Cybersecurity Concepts
Safety/security and effectiveness (sec. 1)
Reduce risk to ensure intended device performance and high level of protection of health (sec. 2, 5, 6, 9)
• In all operation mode
• Intended/reasonable foreseeable risk
Secure Design and Manufacture (sec. 4a)
• Risk management across the life cycle (sec. 3, 14.4, 14.5, 19.3)
• Protection against risk during intended use and reasonable foreseeable misuse (sec. 3c, 8)
• Protection against unauthorised access (sec. 17.4, 18.8)
• Identify threats, vulnerabilities, hazards, risks (sec. 3b)
• Establish risk control measures (sec. 4)
• Minimum IT security requirements (sec. 17.4, 14.5)
Verification/validation (sec. 17.2)
MDR Annex I
Regular updates
State of the art (sec. 1, 4, 17.2)
Acceptable residual risk (sec. 4)
Information for users, instructions and labelling (sec. 4, 23.1, 22.1, 23.4)
Documentation* (sec. 3)
* See also Annex II of MDR

Figure 11. MDR Annex I Requirements on Cybersecurity

Table XX lists the relevant general safety and performance requirements from Annex I of the MDR 2017/745 and IVDR 2017/746 with regard to cybersecurity.

Table 4. Annex I Requirements on Cybersecurity

Main Topic	Section number MDR Annex1	Section number IVDR Annex 1
Device Performance	1	1
Risk reduction	2	2
Risk management system	3	3
Risk control measures	4	4
Minimisation of foreseeable risks, and any undesirable side-effects	8	8
Combination/connection of devices/systems	14.1	13.1
Interaction between software and the IT environment	14.2.d	13.2.d
Interoperability and compatibility with other devices or products	14.5	13.5
Repeatability, reliability and performance	17.1	16.1
Development and manufacture in accordance with the state of the art, taking into account the principles of development life cycle, risk management, including information on security verification and validation	17.2	16.2
Minimum IT requirements	17.4	16.4
Unauthorised Access	18.8	
Lay persons	22.1	
Residual risks: (information supplied by the manufacturer}	23.1.g	20.1.g

Funded by Horizon Europe Framework Programme of the European Union

Main Topic	Section number MDR Annex1	Section number IVDR Annex 1
Warnings or precautions (information on the label)	23.2.m	20.2.m
Residual risks, contra-indications and any undesirable side-effects, (information in the instructions for use)	23.4.g	
Minimum IT requirements: (information in the instructions for use)	23.4.ab	20.4.1.ah

3.3.4 Other Requirement´s Sources

The content of this section is extracted from chapter 6 of MDCG 2019-16 guidance.

At EU level, the following legislative acts are relevant to the cybersecurity of medical devices or to operators dealing with protecting or processing of personal data stored in medical devices and might apply in parallel to the Medical Devices Regulations:

- Network and Information Systems (NIS) Directive[15] . It provides legal measures to boost the overall level of cybersecurity in the EU. See also Annex I of MDCG 2019-16 “Mapping of IT security requirements to NIS Directive Cooperation Group measures”
- General Data Protection Regulation (GDPR) [16]. It regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU.
- Cybersecurity Act [17], [18], [19]. It introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services and processes.

Other cybersecurity guidance can be useful for comparison to find gaps in MDCG 2019-16 guidance:

- US FDA “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions” [20]
- IMDRF Medical Device Cybersecurity Guide [21]

3.3.5 Cybersecurity and Safety Risk Management

Relationship between Processes for Cybersecurity Risk Management and Safety Risk Management

Figure 3.7 is included in Annex IV of MDCG 2019-16 guidance.

Funded by Horizon Europe Framework Programme of the European Union

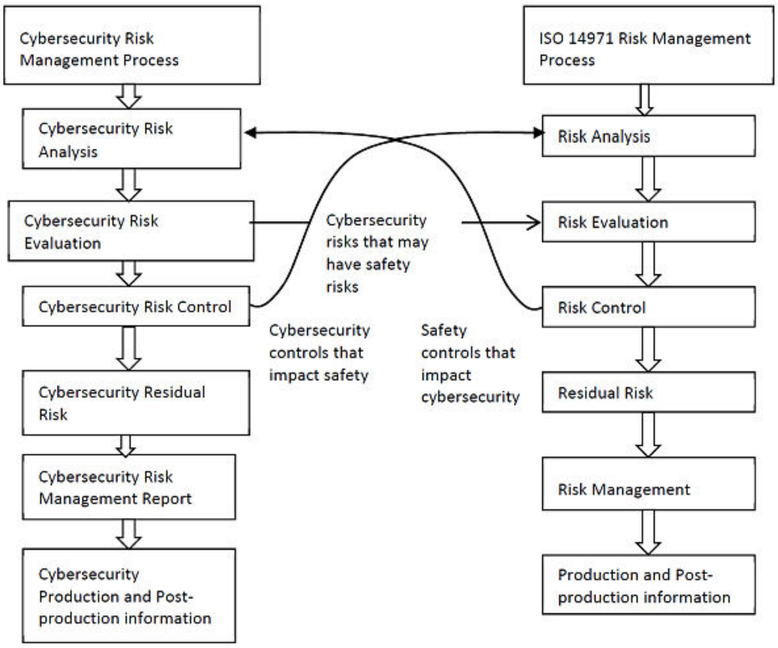

Cybersecurity Risk Management Process
Cybersecurity Risk Analysis
Cybersecurity Risk Evaluation
Cybersecurity Risk Control
Cybersecurity Residual Risk
Cybersecurity Risk Management Report
Cybersecurity Production and Post-production information
ISO 14971 Risk Management Process
Risk Analysis
Risk Evaluation
Risk Control
Residual Risk
Risk Management
Production and Post-production information
Cybersecurity risks that may have safety risks
Cybersecurity controls that impact safety
Safety controls that impact cybersecurity

Figure 12. Relationship between Cybersecurity and Safety Risk Management

3.3.6 Current Services: Data / Services / Processes

- The need for cybersecurity standards is clear:Large volumes of data stored and maintained in healthcare organisations
- Accelerated digital transformation of healthcare systems.
- Healthcare - Top 5 sectors most affected by cybersecurity threats in 2021.
- Threat Groups: Ransomware, Malware, Threats against data, threats against availability
- A methodological and technical cybersecurity framework designed for healthcare services that use Connected Medical Devices (CMDs). Such a framework is aligned with the MDR and IVDR regulations, but strengthens the adherence to requirements concerning safety, performance and IT security. This is also relevant in other domains, and some of the standards mentioned have a multi domain approach.
- In particular, cybersecurity standards will make necessary to:

  1. Identify gaps and introduce new safety and security requirements based on evidence, adapting such requirements to novel technologies (e.g. cloud computing, artificial intelligence)
  2. Identify security-related hazard categories and risk acceptance criteria according to the classification of medical devices

Funded by Horizon Europe Framework Programme of the European Union

3. Promote a risk assessment framework built on risk-benefit analyses that responds to the identified requirements and gaps and considers the impacts of novel scenarios on risks (e.g. safety, performance and environmental differences of in-hospital with respect to, remote monitoring of patients)

4. Provide tools that help mitigate risks and the increase of safety, security and performance of healthcare services relying on CMD /IVD (In Vitro Diagnostic) /SaMD (Software as a Medical Device) with consideration to challenges involving legacy devices.

3.3.7 Other Applicable Standards

Annex III of MDCG 2019-16 includes the following list with other standards than can be relevant:

- EN ISO 14971 Risk Management (Product)
- EN 62304 Software Lifecycle
- EN ISO 31000 Risk Management (Organisation) or particular standards under ISO 31xxx.
- EN ISO/IEC 27000 Information technology — Security techniques — Information security management systems (ISMS) — Overview and vocabulary
- EN ISO/IEC 27001 Information Technology – Security techniques – Information Security management Systems – Requirements.
- EN ISO/IEC 60601-1-x
- IEC 82304-1 Health Software Part 1: General requirements for Product Safety
- ISO/IEC 80001-1 Application of Risk Management for IT networks Incorporating Medical Devices
- ISO/IEC 80001-5-1 Application of Risk Management for IT networks incorporating medical devices – Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 5-1: Activities in the product life-cycle.
- IEC/TR 80001-2-2 Application of Risk Management for IT networks Incorporating Medical Devices Part 2-2: Guidance for the Disclosure and Communication of Medical Device Security Needs, Risks and Controls
- IEC/TR 80001-2-8 Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2
- ISO/IEC 80001-xx including IEC/TR 80001-2-1, IEC/TR 80001-2-3, IEC/TR 80001-2-4,
- IEC/TR 80001-2-5, ISO/TR 80001-2-6, ISO/TR 80001-2-7 or other
- EN ISO 62366 / ISO 60601-4 Usability Engineering
- IEC 62443-4-2 Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components.
- IEC 62443-4-1 Security for industrial automation and control systems. Part 4-1: Secure product development lifecycle requirements.
- IEC/TR 60601-4-5 Medical Electrical Equipment – Part 4-5. Safety related technical security specifications for medical devices.

3.4 CYLCOMED standardisation strategy and plan

The following activities are proposed, to be carried out during the timeframe of the project:

3.4.1 CYLCOMED regular meetings

In April 2024, the first specific WP7 meeting took place (in previous ones WP7 had been handled but not individually) , which dealt with dissemination, standardisation and exploitation activities in CYLCOMED. The purpose of these meetings is to cover the actions to guarantee the impact of the results obtained in CYLCOMED. The team will have monthly meetings, with the participation of MARTEL as WP7 coordinator. As a result of these meetings, specific actions to carry out on (among others) the standardisation activities are defined. The meetings are expected to be very useful as brainstorming sessions and help bring new ideas on the subject.

3.4.2 Seek support from the EU resources.

CYLCOMED is contacting HSbooster.eu (https://www.hsbooster.eu). HSbooster.eu is a 30-month European Commission initiative that will provide the European Standardisation Booster. The booster provides expert services to European projects to help them to increase their time to market.

HSbooster.eu provides complimentary online training sessions designed to empower participants with essential skills and knowledge for effective engagement with standardisation practices, fostering innovation and knowledge valorisation across industries. Partnering with leading experts, researchers, trainers, and standard-developing organisations (SDOs), our Training Academy offers insightful talks, presentations, and real-life experiences in standardisation implementation.

Explore our curated training session catalogue. Elevate your project and achieve success with the HSBooster.eu Training Academy.

Share the insights to boost standardisation teaching for enhanced knowledge valorisation.

3.4.3 Monitoring of Participation of Partners in SDOs

An Excel file has been set up for monitoring the participation of partners in Standards Development Organizations (SDOs). The excel sheet intends to make it possible to add, maintain its content, and define specific actions or follow-ups on the activities. Partners have been asked to update the Excel file continuously, every time they participate in SDOs sessions. Table XX shows the type of information requested.

Table 5. Tracking of standardisation activities

Date	i.e. 15th-04-2024
Type of activity	i.e. Working group meeting
Title	i.e. ref to doc of specific standard

Funded by Horizon Europe Framework Programme of the European Union

Related standard	
Working Group	
Active Party	Member of CYLCOMED
Person involved	(optional)
Summary of activity	Purpose and content
Suggested follow up activities	
Topics discussed that may be relevant for CYLCOMED	
Activities of CYLCOMED relevant to the topics discussed in the standardisation group.	

Hospital Niño Jesús is a member of CEN/TC251 on Health informatics. His contribution in CYLCOMED is providing feedback to standards such as ISO 11073 on cybersecurity subjects.

Please refer to CYLCOMED deliverable XX for more information on the standardisation issues.

We find it important to show that partners are active in standardisation and to foster the exchange between project partners. The results of partners participation will be presented by the end of the project in D7.4.[23]

3.4.4 Training Sessions about relevant standards

The consortium will allocate time and effort on a series of training sessions on relevant standards used in different tools/methods/use cases, in order to bring awareness to CYLCOMED partners about the existence of such standards. Invitations to a standardisation presentation will be sent at least 2 weeks in advance. The purpose is to try to collect as many attending partners as possible. One of the most interesting outcomes of these meetings is to receive feedback from the rest of the partners about the way a standard could be applicable in a particular application, and to promote the active participation of partners in the SDOs. These sessions will be recorded and available for the project partner who could not join and used for dissemination purposes.

The gap analysis (missing points to be considered in the standard current text description) on concepts detailing strengths and weaknesses of the applicable standards will be taken into consideration in the course of the following months. A gap analysis of such standards will be carried out as the training sessions of selected standards are being presented to the CYLCOMED partners. This will allow communication of specific messages to SDOs.

The following activities have been carried out so far:

Date: 05/2024

Title: Standardisation Training Session 1 - CEN ISO/IEEE 11073: Health informatics - Medical / health device communication standards

Video link: https://www.cylcomed.eu/event/cylcomed-training-session-1-on-standardisation/

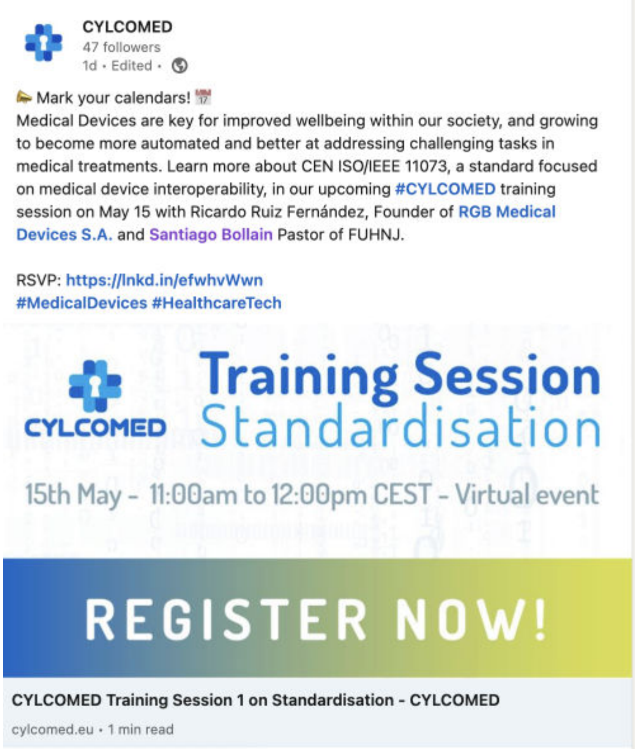
LinkedIn text used for promoting the training session: Mark your calendars!

Medical Devices are key for improved wellbeing within our society, and growing to become more automated and better at addressing challenging tasks in medical treatments. Learn more about CEN ISO/IEEE 11073, a

Funded by Horizon Europe Framework Programme of the European Union

standard focused on medical device interoperability, in our upcoming #CYLCOMED training session on May 15 with Ricardo Ruiz Fernández, Founder of RGB Medical Devices S.A. and Santiago Bollain Pastor of FUHNJ. RSVP: https://lnkd.in/efwhvWwn

X (Twitter) text used for promoting the training session: Mark your calendars! #CYLCOMED is hosting a training session about CEN ISO/IEEE 11073, a standard focused on medical device interoperability on May 15. RSVP: cylcomed.eu/event/cylcomed… #MedicalDevices #HealthcareTech



CYLCOMED
47 followers
1d • Edited •

📣 Mark your calendars! 📅
Medical Devices are key for improved wellbeing within our society, and growing to become more automated and better at addressing challenging tasks in medical treatments. Learn more about CEN ISO/IEEE 11073, a standard focused on medical device interoperability, in our upcoming #CYLCOMED training session on May 15 with Ricardo Ruiz Fernández, Founder of RGB Medical Devices S.A. and Santiago Bollain Pastor of FUHNJ.

RSVP: https://lnkd.in/efwhvWwn
#MedicalDevices #HealthcareTech

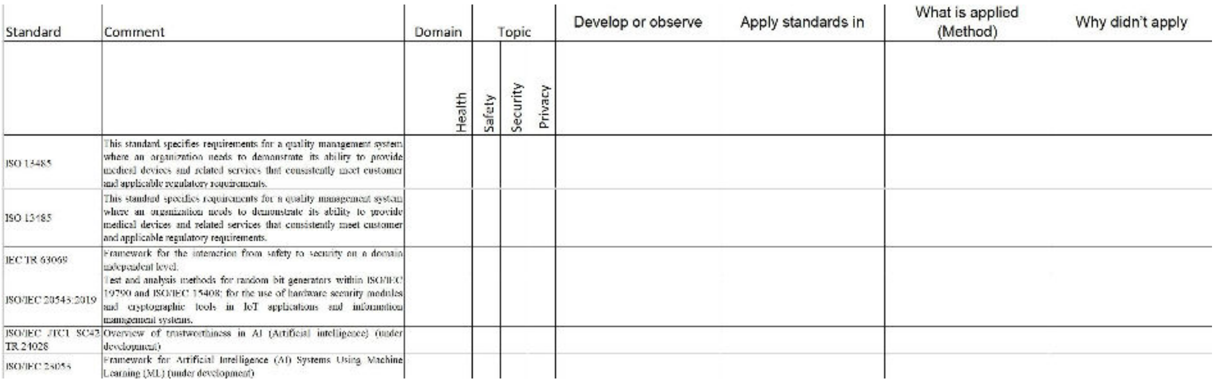
CYLCOMED Training Session 1 on Standardisation - CYLCOMED
cylcomed.eu • 1 min read

Figure 13. Snapshot of the CYLCOMED LinkedIn post

3.4.5 Collection of surveys on standard related issues

Some surveys have been distributed to all partners with the purpose to collect information on the relation of partners with particular standard related issues. It is important to identify their availability to participate/ influence in a particular SDO, in relation to a particular standard. These surveys will be used as a tool in the forthcoming months to gain deeper knowledge on specific standard related issues.

Funded by Horizon Europe Framework Programme of the European Union



Standard	Comment	Domain	Topic			Develop or observe	Apply standards in	What is applied (Method)	Why didn't apply
		Health	Safety	Security	Privacy				
ISO 13485	This standard specifies requirements for a quality management system where an organization needs to demonstrate its ability to provide medical devices and related services that consistently meet customer and applicable regulatory requirements.								
ISO 13485	This standard specifies requirements for a quality management system where an organization needs to demonstrate its ability to provide medical devices and related services that consistently meet customer and applicable regulatory requirements.								
IEC TR 63069	Framework for the interaction from safety to security on a domain independent level.								
ISO/IEC 20543:2019	Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408; for the use of hardware security modules and cryptographic tools in IoT applications and information management systems.								
ISO/IEC JTC1 SC42 TR 24028	Overview of trustworthiness in AI (Artificial intelligence) (under development)								
ISO/IEC 23053	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (under development)								

Funded by Horizon Europe Framework Programme of the European Union

4 EXPLOITATION STRATEGY AND PLAN

Task 7.2 of the project proposal is dedicated to the exploitation actions. Partners are expected to complete certain activities focused on the commercial viability of the main outcomes. It will consider new business and operating models for bringing the project results to customers. For this purpose it must consider how obligations under the new Medical Device Regulations can act as a catalyst to drive demand for cybersecurity tools (covering risk management and security controls) that CYLCOMED will deliver as project results. This task puts a strong focus on how all stakeholders can profit from the exploitation of the results, and develop a timeline for exploitation, identifying the prospective time frame after the end of the project to bring the results to the market. It will manage the IPR, knowledge management and business planning. CYLCOMED, as a research and innovation project. It will explore different types of output:

1) Increased knowledge and expertise which produces "competency impacts";

2) New or increased knowledge that affects the future performance of the related industries;

3) Results which could lead to direct economic benefits (development, creation and marketing of products, services or processes).

A catalogue of the CYLCOMED results will be set up and an exploitation plan at the mid- term of the project, which will be updated at the end of the project. Identification of necessary subsequent research projects, and opportunities for co-funding (at European or National Levels) will be investigated by partners for each key exploitable result identified.

4.1 Exploitation objectives

This deliverable aims to create a business and exploitation plan that will explore the potential for the development and exploitation of the methods implemented after the achievement of the CYLCOMED project. All partners are involved in the exploitation activity by evaluating the potential use, marketability and the applicability of the key concepts and ideas for the evolution of the tools, methods or use cases.

This deliverable is intended to:

- Present a preliminary exploitation plan for the project and provide holistic overview of the exploitation landscape surrounding it;
- Set up a survey to identify the markets and sectors that are relevant in the context of exploitation, and to emphasise the importance of analysing their role, needs and potential;
- Serve as a step towards setting out clear and measurable exploitation targets, whose results will be monitored and reviewed regularly;
- Serve as a guidance document for CYLCOMED project partners and to stimulate exploitation engagement among partners;
- Ensure that exploitable entities will be deployed in an optimal way and that the desired impact is achieved;
- Act as a preliminary document that will be developed further in the following years.

The main objective for exploitation in CYLCOMED is to implement an exploitation strategy to facilitate the successful exploitation and adoption of results and benefits within cybersecurity methods and tools to reduce the time and cost needed to verify and validate automated systems with respect to security requirements.

Funded by Horizon Europe Framework Programme of the European Union

Exploitation is referred to by the EC as the utilisation of results in further research activities other than those by the action concerned or in developing, creating and marketing a product or process, or in creating and providing a service, or in standardisation activities [1].

The meaning of the word "results" in this context is broad, and refers to any tangible or intangible output of the action, such as data, knowledge and information whatever their form or nature, whether or not they can be protected, which are generated in the action as well as any attached rights, including intellectual property rights [1].

The CYLCOMED exploitation and business impact task (Task 6.2) aims to explore and define the potential for the development and exploitation of the project results and to plan the following exploitation process.

Based on this requirement, CYLCOMED aims to address exploitation in a coherent manner throughout the project and to support the beneficiaries in eliciting and coordinating their exploitation strategies, thus increasing the chances for the results of the project to become, through appropriate exploitation measures, innovations that can produce tangible benefits and satisfy specific needs and wants.

The main objective for exploitation in CYLCOMED is to implement an exploitation strategy to facilitate the successful exploitation and adoption of results and benefits within security methods and tools to reduce the cybersecurity risks in CMDs with respect to SCP requirements.

The CYLCOMED exploitation and business impact task (Task 7.2) aims to explore and define the potential for the development and exploitation of the project results and to plan the following exploitation process.

Based on this requirement, CYLCOMED Task 7.2 aims to address exploitation in a coherent manner throughout the project and to support the beneficiaries in eliciting and coordinating their exploitation strategies, thus increasing the chances for the results of the project to become, through appropriate exploitation measures, innovations that can produce tangible benefits and satisfy specific needs and wants.

4.2 Project compromises

- Focus on the main results and their commercial viability. Focus on how all stakeholders can profit from the exploitation of the results.
- Consider new business and operating models.
- Develop a timeline for exploitation.
- Identify concrete customers' needs.
- Start exploitation of intermediate results already during the project.
- Consider non-technical developments.
- Protect intellectual property.

- CYLCOMED partners will identify potential assets to be exploited (with possible joint exploitation strategies) and draft business plans and strategies to gain market penetration in the security and medical field.

- Facilitate the exploitation of the project's outcome and actively promote the further development of innovative solutions based on the CYLCOMED outcomes both for partners and for other EU players.

- Develop and execute an effective exploitation plan with measures during and after the project

- Evaluation of interest from the market, e.g., via questionnaires

- Monitoring of >=6 exploitation KPIs relevant for measures related to joint and individual exploitation by Consortium partners
- Patentability of technologies
- Beta testing demonstrations
- (Potential) agreements with early customers or stakeholders
- Traders recruited
- Spin-Offs created
- Detect new assets
- Contribution to project´s Exploitation, objectives and KPIs
- Respond to Exploitation Survey

Grant Agreement No.: 101095542
Call: HORIZON- HLTH-2022-IND-13
Topic: HORIZON-HLTH-2022-IND-13-01
Type of action: HORIZON-RIA

CYLCOMED

Cyber-security toolbox
for connected medical devices

SURVEY ON EXPLOITATION AND BUSINESS PLAN

Initial Exploitation Activity Report and Short-Long Term Market Analysis

1 SURVEY

Organisation short name	**LOGO**
Organisation type	
Business model	
Expertise	

CYLCOMED will provide a methodological and technical cybersecurity framework designed for healthcare services that use CMDs. As part of our commitment in CYLCOMED project, we must identify the real key exploitable results of each of the consortium partners.

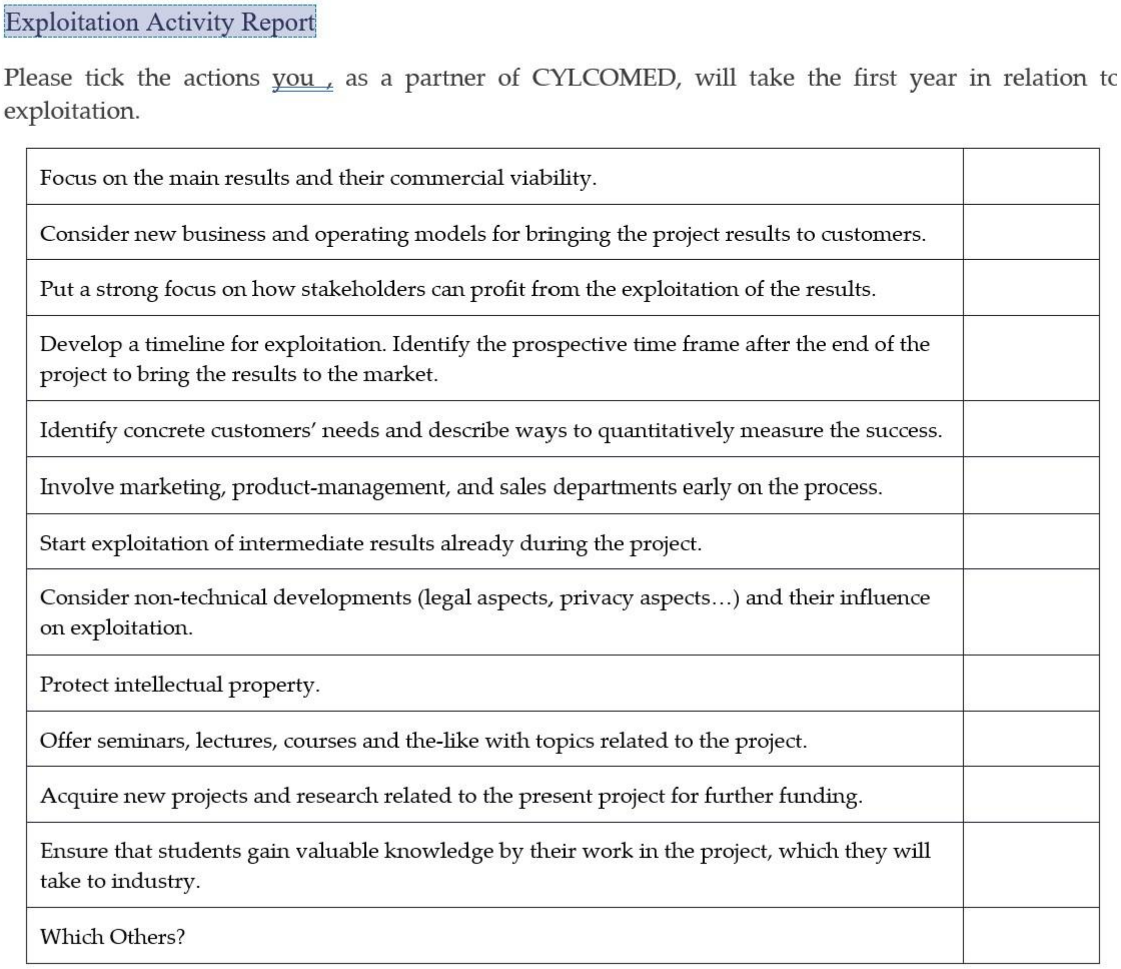
YOUR CONTRIBUTION

Please provide a short response to the following questions (maximum 5 lines).. A business model must provide information on the following elements:

1. **Identification of the key exploitable results (assets) to be obtained by your organization**
   These are the products and/or services the organization offers in order to meet the needs of its customers. A company's value proposition is what distinguishes itself from its competitors.

2. **In case this applies, which year will the result start to be available for the rest of CYLCOMED partners?** (please indicate the exploitable result and the year (1 , 2 or 3).

Funded by Horizon Europe Framework Programme of the European Union

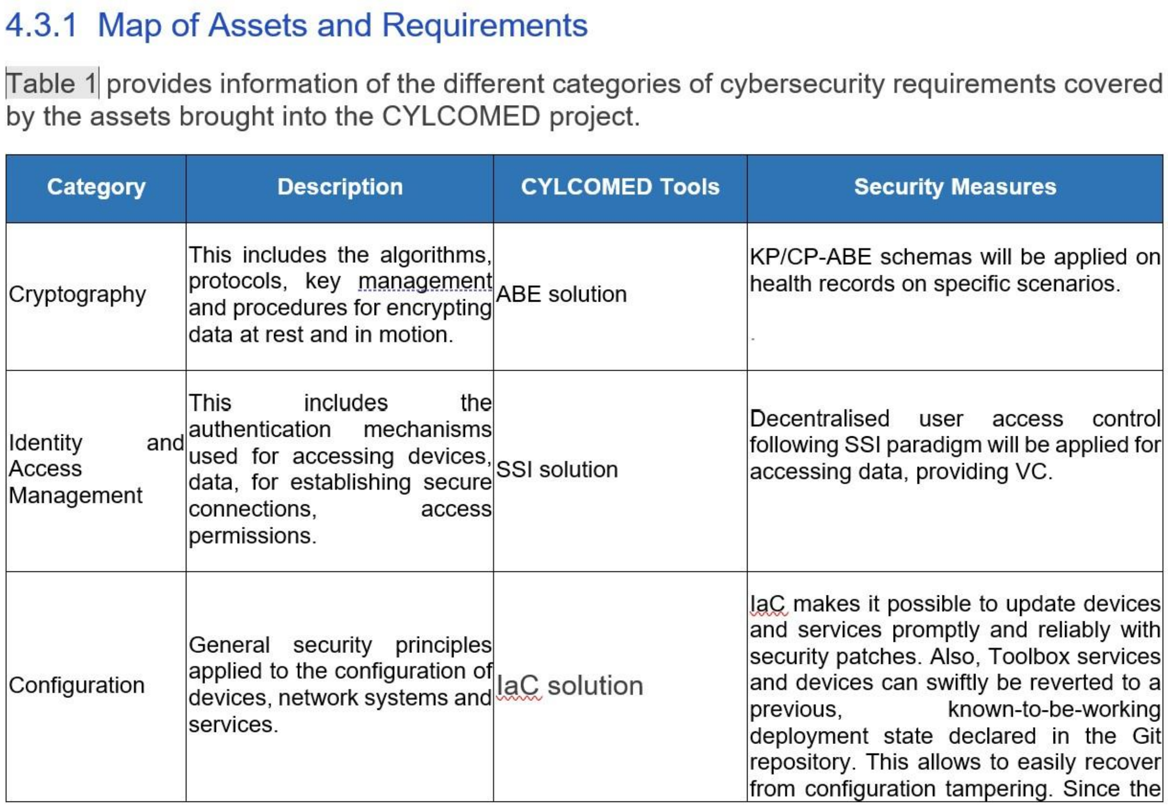


Exploitation Activity Report

Please tick the actions you , as a partner of CYLCOMED, will take the first year in relation tc exploitation.

Focus on the main results and their commercial viability.	
Consider new business and operating models for bringing the project results to customers.	
Put a strong focus on how stakeholders can profit from the exploitation of the results.	
Develop a timeline for exploitation. Identify the prospective time frame after the end of the project to bring the results to the market.	
Identify concrete customers' needs and describe ways to quantitatively measure the success.	
Involve marketing, product-management, and sales departments early on the process.	
Start exploitation of intermediate results already during the project.	
Consider non-technical developments (legal aspects, privacy aspects…) and their influence on exploitation.	
Protect intellectual property.	
Offer seminars, lectures, courses and the-like with topics related to the project.	
Acquire new projects and research related to the present project for further funding.	
Ensure that students gain valuable knowledge by their work in the project, which they will take to industry.	
Which Others?	

-
- CYLCOMED D3.1 Baseline analysis requirements and specifications v2.2



4.3.1 Map of Assets and Requirements

Table 1 provides information of the different categories of cybersecurity requirements covered by the assets brought into the CYLCOMED project.

Category	Description	CYLCOMED Tools	Security Measures
Cryptography	This includes the algorithms, protocols, key management and procedures for encrypting data at rest and in motion.	ABE solution	KP/CP-ABE schemas will be applied on health records on specific scenarios. .
Identity and Access Management	This includes the authentication mechanisms used for accessing devices, data, for establishing secure connections, access permissions.	SSI solution	Decentralised user access control following SSI paradigm will be applied for accessing data, providing VC.
Configuration	General security principles applied to the configuration of devices, network systems and services.	IaC solution	IaC makes it possible to update devices and services promptly and reliably with security patches. Also, Toolbox services and devices can swiftly be reverted to a previous, known-to-be-working deployment state declared in the Git repository. This allows to easily recover from configuration tampering. Since the

4.3 IoT Cybersecurity Market Overview in the Healthcare Sector

The healthcare industry is undergoing a digital transformation, with the widespread adoption of IoT devices promising to revolutionise patient care, improve operational efficiency, and enhance medical outcomes. However, as healthcare organisations embrace connected medical devices and telehealth solutions, they also face unprecedented cybersecurity challenges, necessitating robust measures to protect sensitive patient data and ensure the integrity of medical systems.

4.3.1 Market Growth and Drivers

This section intends to provide an analysis from a business and market point of view over topics (or their associated market segment) relevant to the scope of CYLCOMED framework. Such analysis – and its continuous update - is a core part towards successful exploitation of the project's results, enabling an improved understanding of the associated market segment, the novel solution(s) differentiating features or limitations compared to the ones available in the market, among others.

The IoT cybersecurity market in the healthcare sector is experiencing rapid growth, driven by several key factors:

- Proliferation of Connected Medical Devices: The increasing prevalence of IoT-enabled medical devices, at hospital and home care areas, such as infusion pumps, pacemakers, and wearable health monitors, is expanding the attack surface and heightening the risk of cyber threats targeting patient safety and privacy.

- Remote Patient Monitoring: The adoption of telehealth platforms and remote patient monitoring solutions has surged, especially in response to the COVID-19 pandemic, amplifying the need for robust cybersecurity measures to safeguard sensitive health data transmitted over networked systems.
- Regulatory Compliance Mandates: Healthcare organisations are subject to stringent regulatory frameworks, including HIPAA (Health Insurance Portability and Accountability Act) and FDA (Food and Drug Administration) guidelines, which mandate the implementation of comprehensive cybersecurity measures to protect patient information and ensure regulatory compliance.
- High Stakes of Data Breaches: The healthcare sector is a prime target for cyber attacks due to the valuable nature of patient data, which can be exploited for identity theft, insurance fraud, and other malicious purposes, underscoring the critical importance of mitigating cybersecurity risks.

4.3.2 Key Challenges

Despite the growing demand for IoT cybersecurity solutions in healthcare, several challenges persist:

- Legacy Systems and Infrastructure: Many healthcare organisations operate on legacy IT systems and medical devices that may lack built-in security features or are incompatible with modern cybersecurity solutions, posing significant challenges for securing interconnected networks.
- Interoperability Concerns: The heterogeneity of IoT devices and healthcare IT systems can lead to interoperability issues, making it difficult to implement cohesive cybersecurity strategies that address the unique security requirements of each device and system
- Human Factor: Human error and insider threats remain significant cybersecurity risks in healthcare settings, highlighting the importance of cybersecurity awareness training for healthcare professionals and staff to mitigate the risk of inadvertent data breaches or malicious insider activities.
- Supply Chain Vulnerabilities: The interconnected nature of the healthcare supply chain, encompassing medical device manufacturers, software vendors, and third-party service providers, introduces additional cybersecurity risks, as vulnerabilities in one part of the supply chain can compromise the security of the entire ecosystem.

4.3.3 Market Growth and Drivers

Despite these challenges, the IoT cybersecurity market in the healthcare sector presents promising opportunities for vendors offering innovative solutions tailored to the unique requirements of healthcare organisations. Key trends shaping the market include:

- Supply Chain Vulnerabilities: The interconnected nature of the healthcare supply chain, encompassing medical device manufacturers, software vendors, and third-party service providers, introduces additional cybersecurity risks, as vulnerabilities in one part of the supply chain can compromise the security of the entire ecosystem.

Funded by Horizon Europe Framework Programme of the European Union

- Endpoint Security Solutions: Endpoint security solutions designed specifically for medical devices are gaining traction, offering features such as real-time threat detection, device authentication, and remote monitoring to protect against cyber threats and ensure the integrity of connected medical devices.
- Data Encryption and Secure Communication: The adoption of encryption technologies and secure communication protocols, such as SSL/TLS and VPNs, is essential for safeguarding sensitive patient data transmitted between IoT devices, healthcare IT systems, and cloud-based platforms.
- Zero Trust Architecture: Zero Trust Architecture (ZTA) principles, which assume zero trust for both internal and external network traffic, are increasingly being adopted by healthcare organisations to mitigate the risk of unauthorised access and data breaches in IoT environments.
- Collaborative Partnerships: Collaboration between cybersecurity vendors, healthcare providers, regulatory agencies, and industry stakeholders is crucial for developing cohesive cybersecurity frameworks, sharing threat intelligence, and fostering a culture of cybersecurity awareness and resilience in the healthcare sector.
- In conclusion, the IoT cybersecurity market in the healthcare sector is poised for continued growth, driven by the increasing adoption of connected medical devices, regulatory compliance mandates, and the imperative to protect patient data and ensure the integrity of medical systems. Despite challenges such as legacy infrastructure and supply chain vulnerabilities, innovative cybersecurity solutions and collaborative initiatives hold the key to mitigating security risks and safeguarding the future of connected healthcare.

4.3.4 Market Size

ENISA's recent Cybersecurity Market Analysis framework (ECSMAF) [13,14] has been defined in alignment with Europe's Cybersecurity Act (CSA), including the distinction between supply and demand, or aspects such as the analysis of market and technological trends, supply chain considerations, or socio-economic, policy and regulation aspects.

The size of the IoT market, and the associated number of devices, is only expected to increase according to Globenewswire[1], the IoT Devices market is expected to grow above a Compound Annual Growth Rate (CAGR) of around 10.10% between 2022 and 2028, being estimated to hit approximately US$ 2,724.42 Million by 2028 (compared to US$ 1,529.50 Million in 2021).

Several factors support these predictions, such as a) business pursuit of digitised and automated processes, b) business recovery from disruptions due to COVID-19 (e.g. observed in fleet management, commerce or logistics services), c) further deployment and maturity of 5G networks and supported capabilities and use cases (e.g. massive connectivity of IoT devices) or d) the worldwide competition for leading Artificial Intelligence (AI) technology, which itself depends on the availability of data and thus pushes for new ways of applying IoT (e.g. new sensors and associated devices), just to name a few.

[1] *https://www.globenewswire.com/news-release/2022/09/01/2508413/0/en/With-10-10-CAGR-IoT-Devices-Market-Size-Worth-USD-2724-42-Million-by-2028-Global-IoT-Devices-Industry-Trends-Share-Value-Analysis-Forecast-Report-by-Facts-Factors.html*

Funded by Horizon Europe Framework Programme of the European Union

According to MarketsandMarkets[2]The global IoT security market is expected to grow from 14.9 billion US$ in 2021 to 40.3 billion by 2026, at a Compound Annual Growth Rate (CAGR) of 22.1% during the forecast period. The market is very diverse and competitive, involving the presence of various key players, stemming from distinct sectors, in the ecosystem.

Regulations imposed by the security authorities across North America and Europe have also driven companies to improve IoT security measures, spanning device authentication and management, secure connectivity, or data loss prevention – such as protected data with commercial value, and personal data, scoped within Europe's General Data Protection Regulation (GDPR). Such solutions, integrated within IoT devices, aim at providing real-time protection from threats, preventing or minimising incidents' impact.

The IoT cybersecurity market, similarly to the IT market, has followed a feature-centric path, with security considerations being placed as an after-thought, i.e. as opposed to a "secure-by-design" approach.

Increasingly connected devices are a double-edged sword, empowering businesses (e.g. allowing real-time operational data), while also being susceptible to cyber-attacks. IoT-related cyber-attacks have increased due to (among other reasons) increased digitalization and connectivity, also boosted during the pandemic, which only aggravated IoT-based vulnerabilities (e.g. with prolonged multi-device usage in household settings). Recent projections estimate that the number of IoT devices worldwide is expected to almost triple from 9.7 billion in 2020 to more than 29 billion IoT devices in 2030[3]. Supporting sectors such as education, transport, energy, health and security, further emphasises how threats and risks associated with IoT devices and systems can have huge consequences on both cyber and physical domains. In parallel, the number of attacks and vulnerabilities associated with IoT systems have only increased. Attacks like Mirai[4] highlight that weak security measures in the development, adoption and usage of IoT devices can have a tremendous impact – such as Distributed Denial of Service (DDoS) attacks enabled by the orchestration of a large number of compromised devices.

Some of the main cybersecurity challenges for cybersecurity end users (or vertical sectors) include, from the most generic to the most sector-specific[5]:

- Protecting / avoiding the exposure of sensitive and confidential information (e.g. personal data, internal business records)
- Business or production disruptions or shutdowns resulting from sabotage
- Damage to organisation's reputation and loss of public or customer trust
- Violation of regulatory requirements/potential fines
- Damage to equipment as the result of manipulation or physical events
- Intellectual property theft
- Potential for environmental harm (e.g. utilities sector)
- Potential for humans harm (e.g. eHealth sector)
- Reduced visibility and control due to the complexity of IT systems being connected to

[2] *https://www.marketsandmarkets.com/Market-Reports/iot-security-market-67064836.html*

[3] *https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, published May 2022, accessed 12/8/2022*

[4] *https://www.netscout.com/use-case/weaponization-internet-infrastructure, published July 2020, accessed 12/8/2022)*

[5] *The above list was built from and extended the trending challenges identified for the IoT grid sector market analysis [2]*

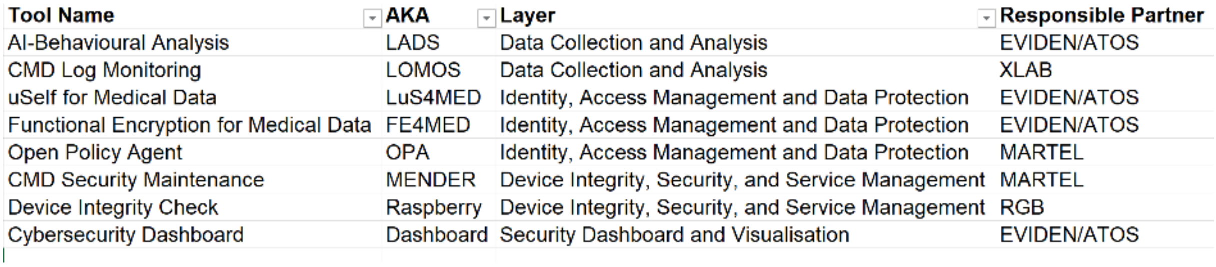
Funded by Horizon Europe Framework Programme of the European Union

OT (Operational Technology) systems (e.g. utilities and manufacturing sectors).

4.4 CYLCOMED Business Potential

4.4.1 Catalogue of the CYLCOMED results

Section 3 of D3.1 “Baseline analysis, requirements and specifications” gives an descriptive overview of each of the asset tools as well as the toolbox architecture in each of the two Use Cases´ scenarios. The Map of assets is shown in the following subsection, and has been extracted from subsection 3.3.1 of D3.1.



Tool Name	AKA	Layer	Responsible Partner
AI-Behavioural Analysis	LADS	Data Collection and Analysis	EVIDEN/ATOS
CMD Log Monitoring	LOMOS	Data Collection and Analysis	XLAB
uSelf for Medical Data	LuS4MED	Identity, Access Management and Data Protection	EVIDEN/ATOS
Functional Encryption for Medical Data	FE4MED	Identity, Access Management and Data Protection	EVIDEN/ATOS
Open Policy Agent	OPA	Identity, Access Management and Data Protection	MARTEL
CMD Security Maintenance	MENDER	Device Integrity, Security, and Service Management	MARTEL
Device Integrity Check	Raspberry	Device Integrity, Security, and Service Management	RGB
Cybersecurity Dashboard	Dashboard	Security Dashboard and Visualisation	EVIDEN/ATOS

A detailed description was already included in deliverable 3.1 and will not be included here again. The tools are also described in deliverables D3.2, 5.1 and D6.1 and will not be described here.

As stated in D6.1, section 1.3.2, the Service Management Tools aim to provide secure management of connected medical devices.

4.4.2 Potential business options for CYLCOMED

There are several examples of operational models which can, from a business scope, be mapped to different CYLCOMED products or services, and respective business models. The following builds on and extends the analysis of how those identified options could be exploited business-wise:

- **CYLCOMED framework as a service**: the first operational option refers to the administration and maintenance of the CYLCOMED framework (and its infrastructure) by an entity (or multiple entities). From a business perspective, in such a case CYLCOMED framework could be offered **as a comprehensive feature-rich cybersecurity solution by a single service provider or resulting from the agreement of multiple solution providers**. CYLCOMED as a service will embed the provisioning of specific hardware (e.g.the RaspBy board) in its offering.
- **Single CYLCOMED plane(s) as a service**: The second operational option refers to the management of different planes (i.e. Security, Trust, Privacy, Identity) by distinct entities, an example being identity provisioning and management services to be provided and managed by a single entity. In this case, the business applicability may

match products or services in already existing IoT cybersecurity market segments (e.g. Identity Access Management, in the Identity Management plane case), with a substantial innovation and differentiation degree in some cases (e.g. Trust Management Plane combining Network-based authorization with Verifiable Credentials, Remote Attestation and Reputation Systems for modelling trust of IoT devices and services).

- **Individual CYLCOMED component(s) as products or services**: The third operational option mentioned is the independent provisioning and management of specific components. The associated offers could again be in the form of products or services, depending on the established revenue model. As in the second option, this case matches more closely the offerings in **existing IoT cybersecurity segments**. This is evident for instance with CYLCOMED components which themselves provide significant self-contained value (e.g. Cyber Threat Intelligence or Reputation System). Most of the identified KERs match this option, thus making it the most likely among all to be materialised.

The final identified operational option refers to intermediate models, combining a subset of components or planes to deliver a product or service; a representative example is that of eSIM-based hardened encryption, where eSIM acts as RooT of Trust for "hardening" the encryption process. Either case depicts innovative offers inserted in already existing IoT cybersecurity market segments.

4.4.3 Business analysis and modelling

The goal of exploitation in CYLCOMED is to ensure the sustainability of the project's results beyond the project's lifetime and to demonstrate how CYLCOMED can influence the EU landscape. Exploitation includes multiple forms:

- **Financial exploitation**, by developing products, projects, or services based on the project results.
- **Research and development**, by engaging new products (EU-funded or sponsored by other sources), based on the experiences gained in the project.
- **Education**, e.g. via course offerings, at the university level or in continuing education.
- **Community-building** around the topics of the project, raising awareness for the problems addressed and the proposed solutions.
- **Knowledge transfer**, from academia to industry, by collaboration or via employees.
- **Contributions to open-source projects and standardisation**, providing public access to the framework and encouraging its broad adoption in commercial and public systems for interested parties.

As a main result, the CYLCOMED project is expected to follow a generic plan, regardless of the domain being worked on, for the industrialization of the newly developed technology and a business plan for future commercial exploitation. This is the base for a draft business plan for future commercial exploitation.

Funded by Horizon Europe Framework Programme of the European Union

4.4.3.1 SWOT analysis

Strengths	Weaknesses
● ToolBox integrating cybersecurity security, privacy, trust and recovery features ● Cybersecurity Tools for trust, security and privacy	● Complexity associated with integration into a holistic platform ● Uncertain or variable time to market
Opportunities	Threats
● Hospital/Home Care domains to which CYLCOMED can be applied ● Funding opportunities to enhance CYLCOMED framework maturity ● Increase in high-impact cybersecurity incidents & threats increases the demand for frameworks like CYLCOMED	● Emergence of competing / champion solutions ● Valley of death

Figure 14. Initial CYLCOMED SWOT analysis

4.4.3.2 PESTLE analysis for CYLCOMED ToolBox

PESTLE (Political, economical, social, technological, legal, environmental) analysis assesses a market, including competitors, from the standpoint of a particular proposition or a business. This section provides this analysis from two perspectives:
1 – the CYLCOMED ToolBox (cybersecurity-related business perspective),
2 - the IoT services / applications it has been applied and validated in (IoT service business perspective).

Table 6. PESTLE analysis for CYLCOMED ToolBox

Political - Increasing political instruments to support cybersecurity solutions (e.g., EU Digital Single Market) - Insufficient use of cybersecurity certification of products, services, and processes - Insufficient international cooperation between countries	**Economical** - Severe inflation worldwide Tight European monetary policy - The economic impact of cyberattacks may influence the development and adoption of new cybersecurity solutions by market players
Social - Aftermath of COVID-19 pandemic and increased digitalization - Lack of qualified cybersecurity skilled personnel - Increased awareness around general users around the need for cybersecurity measures and solutions	**Technological** - Worldwide acceleration of AI research & deployment across different sectors and products - Generalisation of Cyber Attacks. Over the past years there has been a significant broadening of scope and diversity to cyber-attacks.

Legal - Europe's Cybersecurity Regulation Act (CRA) brings new cybersecurity product compliance requirements	**Environmental** - Green Bonds as incentive for further adoption of IoT devices

4.4.3.3 PESTLE analysis for CYLCOMED IoT applications/services

Table 7. PESTLE analysis for Medical IoT service (Domain C)

Political - Increasing political instruments to support cybersecurity solutions (e.g., EU Digital Single Market) - Insufficient use of cybersecurity certification of products, services, and processes - Insufficient international cooperation between countries	**Economical** - Severe inflation worldwide Tight European monetary policy - The economic impact of cyberattacks may influence the development and adoption of new cybersecurity solutions by market players
Social - Aftermath of COVID-19 pandemic and increased digitalization - Lack of qualified cybersecurity skilled personnel - Increased awareness around general users around the need for cybersecurity measures and solutions **Legal** - Europe's Cybersecurity Regulation Act (CRA) brings new cybersecurity product compliance requirements	**Technological** - Worldwide acceleration of AI research & deployment across different sectors and products - Generalisation of Cyber Attacks. Over the past years there has been a significant broadening of scope and diversity to cyber-attacks. **Environmental** - Green Bonds as incentive for further adoption of IoT devices

4.5 Consortium exploitation plan

The first step of the process is intended to support the partners in identifying the exploitable results they are interested in and in defining their exploitation strategy. Likewise, it also intends to carry out a preliminary analysis of each of the tools/methods/use cases that will be addressed in the project through a Canvas business model. A specific survey for data collection has been designed for this purpose by the team in charge of the exploitation task (RGB) and shared with the other partners.

After identifying the contribution that each participating entity intends to provide in the implementation of this initial exploitation plan, information will be collected in the following months from each of the companies. This information, as aforementioned, will be updated and worked on in greater depth throughout the project, as the methodologies addressed are detailed.

Funded by Horizon Europe Framework Programme of the European Union

This process is based on questionnaires that aim to cover all the fields in which CYLCOMED parties contribute, so that the information obtained is structured and detailed identically for each of the contributors. The document is a specific document where each contributor is asked to identify which results of the project they consider exploitable, as well as their market-oriented activities. The second document is a study of the specific tools/methods/use cases that will be worked on during the project. In order to structure all the individual exploitation strategies of Task 7.2 contributors, and support the partners in better describing their strategy according to the domain they intend to address, they are requested to declare:

CYLCOMED will provide a methodological and technical cybersecurity framework designed for healthcare services that use CMDs. We are interested to identify the real key exploitable result of each of the consortium partners.

The methodology to be followed for the individual market analysis of each of the CYLCOMED partners is based on:

1. Identification of the results (assets) that each partner will obtain
2. the market share that the organisation will cover
3. the market analysis for that market share
4. The key market drivers, market trends, target user profiles (their interests and preferences), the competitors that your organisation will have
5. what value will their value proposition is compared to yours
6. Which stakeholders should be analysed.

4.5.1 Seek support from the EU resources.

CYLCOMED is contacting HSbooster.eu; This service is divided in two main streams addressing Dissemination & Exploitation strategies, activities and goals. The aim of Dissemination services (Module A and B) is to strengthen the capacity of Project Groups (PGs) in disseminating, maximising the dissemination of a portfolio of results and offering a wider and more complete view to potential users. The aim of Exploitation service (Module C) is to support single projects in exploiting their research results and enhance beneficiaries' capacity to improve their exploitation strategy

(https://www.horizonresultsbooster.eu/ServicePacks/Details/6)

4.5.2 Regular Meetings

In April 2024, the first WP7 meeting took place, which dealt with dissemination, standardisation and exploitation activities in CYLCOMED. The purpose of these meetings is to cover the actions to guarantee the impact of the results obtained in CYLCOMED. The team will have monthly meetings, with the participation of MARTEL as WP7 coordinator. As a result of these meetings, specific actions to carry out on (among others) the standardisation exploitation are defined. The meetings are expected to be very useful as brainstorming sessions and help bring new ideas on the subject.

Funded by Horizon Europe Framework Programme of the European Union

4.5.3 Map of Assets and Requirements

Table 1 provides information of the different categories of cybersecurity requirements covered by the assets brought into the CYLCOMED project.

Category	Description	CYLCOMED Tools	Security Measures
Cryptography	This includes the algorithms, protocols, key management and procedures for encrypting data at rest and in motion.	ABE solution	KP/CP-ABE schemas will be applied on health records on specific scenarios. .
Identity and Access Management	This includes the authentication mechanisms used for accessing devices, data, for establishing secure connections, access permissions.	SSI solution	Decentralised user access control following SSI paradigm will be applied for accessing data, providing VC.
Configuration	General security principles applied to the configuration of devices, network systems and services.	IaC solution	IaC makes it possible to update devices and services promptly and reliably with security patches. Also, Toolbox services and devices can swiftly be reverted to a previous, known-to-be-working deployment state declared in the Git repository. This allows it to easily recover from configuration tampering. Since the Git repository is the "single source of truth", it is also possible to automatically detect misconfigured services or devices. Moreover, besides the system administrator, no one else needs to have access to devices and services, thus dramatically reducing attack surface.
Design	This includes design principles applied to the device/network/service.	ABE solution IaC solution	Modular design and privacy by design is applied on ABE solution. IaC automation shortens deployment time and ensures reproducibility of deployment states. This makes it possible to update devices and services promptly and reliably with security patches. In turn, reproducibility dramatically reduces the time needed to recover from severe production incidents caused by faulty deployments or security breaches as Toolbox services and devices can swiftly be reverted to a previous, known-to-be-working deployment state declared in the Git repository.

Category	Description	CYLCOMED Tools	Security Measures
Secure Communicatio n	Considerations that must be taken into account when establishing connection, exchanging information and allowing connection.	IaC solution	IaC components connect to devices and cloud services using mutual TLS.
Software Security	Measures taken into account to make the software secure.	Security Dashboard AI-based Behavioural Analysis	By developing a correlation engine to process the events and raise security alarms when a threat is detected, the Security Dashboard contributes to software security. The AI-based Behavioural Analysis component uses AI and Machine Learning technologies to model normal behaviour and detect abnormalities, it indirectly contributes to making the software more secure.
Monitoring	Includes every monitoring system used to monitor device/service/system accesses, performances, behaviour, configuration, changes of credentials, etc.	ABE solution SSI solution IaC solution Security Dashboard AI-based Behavioural Analysis	ABE service activity audit log. Authentication activity audit log. The Git repository is the "single source of truth", so it is possible to automatically detect misconfigured services or devices because their runtime configuration would be different than that in the Git repository. Also, the Git repository stores information about who modified the platform state when, thus furnishing an audit trail. The Security Dashboard will provide an integrated view of all security events generated by the various tools within the CYLCOMED toolbox. It will consolidate monitoring systems for device/service/system accesses, performances, behaviour, configuration, changes of credentials, etc. The main functionality of the AI-based Behavioural Analysis component, revolves around monitoring the logs generated by Connected Medical Devices (CMDs) or the platform that manages CMDs, which is a core component of security monitoring
Integrity	Measures to maintain data/device/system/service integrity.	IaC solution AI-based Behavioural Analysis	IaC reproducibility allows recovery from production incidents caused by faulty deployments or security breaches as Toolbox services and devices can swiftly be reverted to a previous, known-to-be-working deployment state declared in the Git

Category	Description	CYLCOMED Tools	Security Measures
			repository. Since the Git repository is the "single source of truth", it is also possible to automatically detect misconfigured services or devices. By identifying anomalies in logs due to attacks or failures, the AI-based Behavioural Analysis component indirectly contributes to the maintenance of data/device/system/service integrity. It facilitates the detection of events that could potentially compromise the integrity of the system
Availability	Measures to maintain data/device/service/system available for authorised use.	IaC solution Security Dashboard	Automated, version-controlled service delivery dramatically reduces the time needed to recover from severe production incidents caused by faulty deployments or security breaches. Thus, IaC plays a role in increasing overall system availability. By providing a real-time graphical representation of detected threats, the Security Dashboard tool ensures that important security information is always available for authorised use
Data protection mechanisms	Mechanisms to maintain data secured.	ABE solution SSI solution Security Dashboard	Data encryption by ABE schemes Decentralised authentication mechanisms for accessing data The Security Dashboard tool will normalise, enrich, and process the security events, which are measures taken to protect the data collected and used by the tool itself
Privacy	Measures to protect data privacy.	ABE solution	Use of Privacy Enhanced techniques (ABE) for protecting user data privacy

Table 8. Requirements Mapping

4.5.4 Results identification for every partner

A second survey document will ask each use case leader (and their contributors) to identify the key partnerships, key resources, key activities, value propositions, customer relationships, channels, customer segments, cost structure and revenue streams of their use case. The collected information will take into account the fact that deliverables 7.3 and 7.4 are “public”.

Funded by Horizon Europe Framework Programme of the European Union

The second step of the methodology will be dedicated to consolidating the exploitation strategy of the project. In this phase, the exploitation plans will be revised and updated at individual level, based on the collected information.

The output produced at the end of the process will be the final exploitation activity report and short/long-term market analysis presented in M36, at the end of the CYLCOMED project.

4.5.5 Joint Exploitation efforts

4.5.5.1 Overview of joint exploitation options

One of the main objectives of the project itself is to extend its lifespan beyond its end; the consortium partners face the challenge of joint exploitation. This commitment has strong dependencies on strategic decisions of the partners' organisations and in this initial report we will describe the draft consortium approach to this joint exploitation. The following months will help to identify the joint exploitation possibilities among partners

In order to reach the necessary decisions, it is key to have open discussions in order to identify each partner's interests and try to preserve the engagement or to look for alternatives that could fill a potential gap.

The key topics to discuss and agree include:

- IPR (Intellectual property rights) / Partner compensation
- Legal structure/consortium agreement
- Commercial agreement

Several scenarios can be envisaged at the end of the project:

1. All consortium partners commit to a joint exploitation of CYLCOMED.
2. Not all partners commit to the joint CYLCOMED solution. Multilateral agreements can be reached between partners to exploit individual components or groups of them that can provide a service or cover a market segment need.
3. Each partner wants to exploit their components individually.
4. Bilateral (multilateral) partners' agreement can be reached to exploit a group of components that can offer one or several functionalities to the market.

All these options will be presented to partners for comments and discussion and decisions will come to action during Y2 and Y3 of the project.

4.5.5.2 IPR

During this first part of the Exploitation and sustainability task (M18), the consortium partners have been working in the generation of a document which will help to protect the intellectual property rights (IPR) of the project results and subsequently support a potential benefit distribution in any future commercial action (including this IPR distribution in the compensation schemes of the commercial opportunity).

The rationale behind this document is to coordinate and agree the distribution (in %) of the IPR ownership that each party claims, in relation to the components/assets (developments susceptible to be commercialised).

This distribution can be:

- A sole partner has developed the component (owner of the 100% of the IPR).
- Several (two or more) partners contributing (% distributed among all co-owners based on their individual efforts).

If it makes sense, this document will be generated and comments to partners will be requested. A draft version will be presented for validation to all partners and included in the next report as part of the annexes.

Table 9. Structure of the IPR distribution table

Name of componente	Lead developer	Contributing parties	IPR %

4.5.5.3 Legal structure

By the time this document is written, there is no official consensus in the consortium to create or set up a new legal structure of any of the main possible legal partnership structures, namely:

- New Legal Entity or Foundation: a new legal entity responsible for any of the commercial operations.
- Joint Venture: a business agreement in which two or more partners acting together and sharing resources in pursuit of a business or in relation to a specific project.
- Supply Chain: consists of a number of partners that contribute for the delivery of a component, product or service with no central structure.

Regardless of all the possibilities available, the consortium must consider if this approach (to create a new legal structure) is viable and could be an efficient vehicle to transfer to the market the project results.

4.5.5.4 Commercial agreement

An intermediate solution, also under discussion, is a commercial collaboration under the form of an Exploitation/Commercial Agreement between consortium partners (two or more partners). This agreement will support any potential commercial opportunity that may appear in the future. The agreement could contribute in will describe in detail the different roles and responsibilities of each of the participants in the event of a commercial opportunity. The idea is that a Service is requested and considered as a target of a business opportunity. In this case, the CYLCOMED platform could be licensed to provide these services. The partners would contribute in accordance to the the IPR distribution of assets/components.

This Exploitation Agreement could include the IPR agreement % by each partner and describe the benefits distributions for all the participants in a commercial opportunity.

This agreement is also in the generation phase and will need to be reviewed by all partners. If considered helpful, it could be used as a template to participate in any potential commercial opportunity that may appear in the future.

A draft version will be presented for validation by all partners in Y2 and included in the next report due by M36 as part of the annexes.

5 CONCLUSIONS

This deliverable on Dissemination, Communication, Standardisation, and Exploitation Strategy and Plan demonstrates the CYLCOMED project's commitment to effectively disseminate its outcomes, foster communication among stakeholders, engage in standardisation efforts, and lay the foundation for successful exploitation of its results.

The project has established robust communication mechanisms, utilising a range of tools and platforms to engage stakeholders, provide regular updates, and encourage dialogue within the field. Through a dedicated project website, newsletters, social media, and press releases, CYLCOMED effectively communicates its progress, achievements, and the significance of its work to a broader audience.

Furthermore, the project has recognized the importance of standardisation and has actively engaged in relevant standardisation groups. By identifying and assessing applicable standards, proposing improvements, and participating in standardisation activities, CYLCOMED has contributed to shaping industry standards and ensuring the alignment of its cybersecurity framework with existing regulations and requirements.

Looking ahead, the project has laid the groundwork for successful exploitation and commercialization of its results. By developing an exploitation strategy, conducting market analyses, and identifying key exploitable results, CYLCOMED partners are well-positioned to leverage their research outcomes and drive their adoption in the market. The project's focus on business planning, intellectual property management, and the identification of subsequent research opportunities further reinforces its commitment to realising the full potential of its results.

By effectively disseminating its outcomes, engaging stakeholders, contributing to standardisation efforts, and preparing for exploitation, the project is poised to make a significant impact on the cybersecurity of Connected Medical Devices. Through its collaborative efforts, CYLCOMED aims to enhance patient safety, protect healthcare infrastructure, and drive innovation in the field of medical device cybersecurity.

Funded by Horizon Europe
Framework Programme of the European Union

REFERENCES

Relevant documents:

[1] International Organization for Standardization (ISO), «ISO 26262-10. Road vehicles — Functional safety — Part 10: Guidelines on ISO 26262,» 2018.Authors, Title2, Date….

[2] International Organization for Standardization (ISO), «ISO 14971. Medical devices — Application of risk management to medical devices,» 2019.…

[3] International Organization for Standardization (ISO), «ISO 14971. Medical devices — Application of risk management to medical devices,» 2019.

[4] ISO 14971, «ISO 14971:2019,» 2019. [En línea]. Available: https://www.iso.org/standard/72704.html.

[5] IEC 60601-1-12:2014/AMD 1, «IEC 60601-1-12:2014/AMD 1:2020,» 2020. [En línea]. Available: https://www.iso.org/standard/78215.html.

[6] IEC 62304, «IEC 62304:2006,» 2006. [En línea]. Available: https://www.iso.org/standard/38421.html.

[7] IEC 62366-1, «IEC 62366-1:2015,» 2015. [En línea]. Available: https://www.iso.org/standard/63179.html.

[8] MDCG, «MDCG 2019-16 Rev.1,» 2019. [En línea]. Available: https://ec.europa.eu/health/system/files/2022-01/md_cybersecurity_en.pdf.

[9] European Commission, "Funding & tenders." [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/glossary. [Accessed: 25-Jun-2020].

[10] MedTech Europe, "The European Medical Technology industry - in figures," *MedTech Eur. - from diagnosis to cure*, p. 44, 2019.

[11] A. Joyce and R. L. Paquin, "The triple layered business model canvas: A tool to design more sustainable business models," *J. Clean. Prod.*, vol. 135, pp. 1474–1486, 2016.

[12] A. Ovan, "What is a business model?," *Harv. Bus. Rev.*, no. January, pp. 1–9, 2015.

[13] ENISA's Cybersecurity market analysis framework: https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf

[14] EU Cybersecurity market analysis - IoT in distribution grid: https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid

[15] Regulation of the European Parliament and of the Council, «Directive (EU) 2022/2555 (NIS2). Measures for a high common level of cybersecurity across the Union,» 2022.

[16] Regulation of the European Parliament and of the Council, «Regulation (EU) 2016/679. General Data Protection Regulation (GDPR),» 2016.

[17] European Commission, «The EU Cybersecurity Act,» [En línea]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

[18] European Commission, «The Cybersecurity Act strengthens Europe's cybersecurity,» [En línea]. Available: https://digital-strategy.ec.europa.eu/en/news/cybersecurity-act-strengthens-europes-cybersecurity.

Funded by Horizon Europe Framework Programme of the European Union

[19] European Commission, «Questions and Answers - EU Cybersecurity,» [En línea]. Available: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369.

[20] Food and Drug Administration (FDA), «Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions,» 2022.

[21] International Medical Device Regulators Forum (IMDRF), «IMDRF/CYBER WG/N60. Principles and Practices for Medical Device Cybersecurity,» 2020.

[22] CYLCOMED Project: D7.1. Dissemination, Communication and Exploitation Strategy and Plan

[23] CYLCOMED Project: D7.2. Dissemination, Communication, Standardisation and Exploitation Initial Report

[24] CYLCOMED Project: D7.3. Dissemination, Communication, Standardisation and Exploitation Final Report (This deliverable)

[22] CYLCOMED Project: D7.1. Dissemination, Communication and Exploitation Strategy and Plan